2011

Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU:

Individual Reports of Testing of 9 Social Networking Sites

By request of the European Commission under the Safer Internet Programme

European Commission
Information Society and Media

VERÓNICA DONOSO

August, 2011

August 2011

Please cite as follows:

Donoso, V. (2011). Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU. Individual Reports of Testing of 9 Social Networking Sites. European Commission, Safer Internet Programme, Luxembourg.

TABLE OF CONTENTS

OVERVIEW OF SIGNATORIES AND TESTERS

This part consists of the reports submitted by the national researchers on each signatory Social Networking Site tested in this phase. Below is a summary of the participating Social Networks, the date of submission of their self-declarations (SD), the language version tested, and the name and affiliation of the tester. For further information on the methodology and testing details please refer to the first part of this report and the annexes.

Signatories	Date of accession to the Principles	Date of submission of the self-Updated self-declarations	Version	Tested by	Affiliation
Dailymotion	10 February 2009	10 November 2010	French	Cédric Fluckiger	University of Lille
Habbo Hotel (Sulake)	10 February 2009	05 November 2010	Finnish English	Niina Uusitalo Jo Bryce	University of Tampere University of Central Lancashire
Stardoll	27 August 2010	27 August 2010	English	Brian O'Neill	Dublin Institute of Technology
Skyrock	10 February 2009	*05 November 2010*	French	Cédric Fluckiger	University of Lille
Windows Live (Microsoft Europe)	10 February 2009	05 November 2010	English	Brian O'Neill	Dublin Institute of Technology
Xbox Live (Microsoft Europe)	10 February 2009	05 November 2010	English	Brian O'Neill	Dublin Institute of Technology
Flickr	10 February 2009	28 November 2010, with minor corrections made on 15 July 2011	English	Jo Bryce	University of Central Lancashire
Yahoo! Pulse	10 February 2009	28 November 2010	English	Jo Bryce	University of Central Lancashire
YouTube (Google)	10 February 2009	05 November 2010	English	Brian O'Neill	Dublin Institute of Technology

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
DAILYMOTION

Cédric Fluckiger, University of Lille 3, France
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Dailymotion is a French video sharing platform. It was launched in March 2005. It exists in more than 20 languages. Dailymotion is not a typical Social Networking Site (SNS), although some of the functionalities present on SNSs may be found here. For instance, registered users have a profile containing some basic information (gender, age, town...); users can also post videos on the platform and if they wish, they can subscribe to other users` videos or ask them to become friends. However, as Dailymotion is primarily dedicated to video sharing and posting, these mechanisms are not prominent on the site. There is no minimum age requirement to sign in as a user on the platform.

Summary of main findings

Dailymotion has clear, age-appropriate safety information targeted at children, parents and educators, accessible from the "child protection" (protection de l'enfance) link from the page footer. In this "child protection" page, several links lead to organizations dedicated to child protection. As Dailymotion is a video platform and not a typical SNS, the users` profiles do not contain much personal information and the profile management page clearly indicates whether every information field is public or private ("public data" or "private data"). Regarding the videos posted on one's profile, users have the option to upload their videos as "private". This option can be chosen during the upload or at any time after publication. Any video set as "private" has a dedicated private URL shown under the player. This URL can be shared with anyone the user wishes to share their video with (including friends and non friends). No highly inappropriate or illegal content (e.g. pornography or very violent content) was found on Dailymotion. Some kind of fictional gory content (e.g. mild or light violence) was found, but it was not easily accessible. On Dailymotion there is a "sexy" non-pornographic channel containing erotic videos, but "explicit content" from this channel is not accessible to logged-in users registered under 18. Arguably, one of the main weaknesses of the site is the fact that the available "family" filter that restricts access to potentially "inappropriate" content, including "explicit content" could easily be set to "off". By default the filter is set to "on" for all users. However, if minors click on a video labelled as "explicit content" they cannot at first access the video and a message stating that users under 18 cannot watch the video is displayed. The message, however, also prompts minors to modify their date of birth if they wish to watch the video and provides a direct link to their profile page where they can easily change their date of birth to one above 18. By doing this, minors (now registered as "adults") are granted access to "explicit content" including the videos that the minor had been unable to access when the family filter was set to "on". Furthermore, because all non-registered users (including minors) can turn the family filter "off" without having to verify their age, it is also possible for minors to disable the family filter by simply turning the family filter to *"off"* before logging into the site.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

The self-declaration states that a dedicated page on child safety for parents and children is provided under the link "child protection" in the site footer. It also states that Dailymotion provides educational videos for young

people about surfing the Internet safely and responsibly including specific tips such as being careful with the personal information one shares online or reporting inappropriate content users may come across. The provider further claims that "the Safer Internet programme in France (internet Sans Crainte) has a Dailymotion account where it uploads videos describing best practices and safe conduct on the internet". The website, thus, provides guidance specifically *targeted* at children and young people on how to navigate their website safely. The signatory claims to provide clear information about what constitutes inappropriate behaviour on their service and the consequences thereof through the Terms of service. Some examples of inappropriate behaviour are uploading pornographic material or photos and videos of people without their permission, not respecting intellectual property, etc. The "Terms" also clearly specify that users` access to their personal page may be temporarily or permanently suspended if they fail to comply with the Terms. In more serious cases (e.g. if someone uploads pornographic material) users` accounts may be deactivated or terminated. Apart from the Terms the provider claims to provide this information in the FAQ which contain information on community features, copyright and privacy policy.

The self-declaration does not mention if Dailymotion offers parents and/or teachers any technical controls on the website.

Main findings in relation to the website

The site contains safety information for children, as well as a shorter version of the Terms of Use ("conditions d'utilisation"). Both the safety information and the shorter version of the Terms of Use are accessible from the "child protection" page ("protection de l'enfance"), in the "legal" ("légal") section, accessible from the footer. This information is easy to find. Safety information contains advice for parents, educators, as well as for children. It also includes links to organizations dedicated to child protection on the Internet (e-enfance, NetEcoute, Safer Internet, etc.). However, only one short paragraph is directly targeted at children. It contains clear and understandable information, though. Besides this, one video, provided by the organisation" Internet sans crainte" is specifically dedicated to children (Safer Internet Day video). Apart from safety material targeted at children, Dailymotion also provides safety Information (including some videos and general advice such as *"we encourage parents to talk to their children*") targeted at parents and educators. This information is comprehensive and easy to understand. On several pages throughout the site it is made clear what content and what types of behaviour are not acceptable on Dailymotion. Furthermore, Dailymotion assures parents that the site provides *"all the tools necessary for a safe* (online) *experience*" and they also provide a contact form to get in touch with the support team.

In the "legal" ("légal") section, one can also find the key points from the terms of use ("conditions d'utilisation"), written in legal style, yet, accessible to children. When registering, a child receives a dedicated email, different to the one addressed to adults. A very clear and complete message is added to the email, including what users can do and what they should not do on the website. Children are warned that some information is public on the platform and they are encouraged not to share personal data.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

According to the self-declaration, Dailymotion employs mechanisms such as video tagging to ensure the limited exposure to potentially inappropriate content and contact by children. The provider claims that videos tagged with keywords in the Dailymotion "blacklist" are "pre-emptively placed behind the Family filter" and are reviewed by the support team to make sure no inappropriate content (e.g. explicit adult content) is uploaded to the site. Dailymotion also claims that the Family filter ("on" by default) prevents users from finding and watching explicit content such as sexy videos or pornographic materials on the service. According to the provider, users logged-in as under 18 cannot deactivate the filter.

Even though the self-declaration states that "Dailymotion works to identify underage users", no minimum registration age is mentioned in the self-declaration and no specific measures regarding how minors are identified and eventually deleted from the site are stated. The self-declaration does mention, though, that users under 18 are "excluded from member search results and users cannot be searched by age". Registered

minors receive an e-mail that reminds them of the different features on Dailymotion (e.g. commenting on other`s videos) and asks them to watch a video on e-safety (the e-enfance video) with their parents.

Regarding the functionalities put at the disposal of content providers, partners or users in order to label, rate or age restrict content where appropriate, the provider states that users can moderate the content submitted to the groups they administrate and they are also given the possibility to flag inappropriate content by clicking on the "report" button placed beneath each video.

Main findings in relation to the website

On Dailymotion, there is no minimum age requirement. All users can register with their actual date of birth. According to the self-declaration, Dailymotion provides a Family filter ("*on*" by default) that prevents users from watching explicit content such as erotic videos or pornographic materials. Tests confirmed that the so-called "family filter" (*"filtre parental")* is set to "*on*" by default. When set to "*on*", the filter prevents users from accessing "explicit content", for instance most videos in the "sexy" category, a channel that displays videos tagged as "sexy" and whose content is "erotic" and/or sexually explicit. Tests, however, also demonstrated that children can set the "filter" to "off" by modifying their registration age to one above 18. By default the filter is set to "on" for all users. However, if minors click on a video that is labelled as containing "explicit content" they cannot at first access the video and a message stating that users under 18 cannot watch the video is displayed. The message, however, also prompts minors to modify their date of birth if they wish to watch the video by stating: *"You must be logged in, over 18 years old, and set your family filter "off" in order to watch it. Please setup your birth info in your profile".* This message provides a direct link to the minor's profile page where they can easily change their date of birth to one above 18. By doing this, minors (now registered as "adults") are granted access to "explicit content" including the videos that the minor had been unable to access when the family filter was set to "on". Moreover, because all non-registered users (including minors) can turn the family filter "off" without having to verify their age, it is possible for minors to disable the family filter by simply turning the family filter to *"off"* before logging into the site.

Regarding the mechanisms available for users to label, rate or restrict content, it is easy for users to label their own videos by choosing the "category" to which the video belongs (e.g.: art, friends and family, politics, animals, cinema, music, sexy, etc.). All these categories are available to all users. However, videos labelled as containing "explicit content" are not accessible to users whose family filter is set to *"on"*.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

As claimed in the self-declaration, Dailymotion provides several tools to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct. According to the provider, users under 18 are "excluded from member search results and users cannot be searched by age" while users of any age are able to "control their personal information and their interactions with other users", for instance, by setting their personal information to "private". Besides, users can also reject friends 'requests, block other users, delete unwanted comments on their profiles, block commenting on their videos, etc. Users can also moderate the content submitted to the groups they administrate and can report inappropriate content on the website.

As mentioned in the self-declaration, "Dailymotion takes an active role in raising children`s and parents `awareness of internet risks". As a matter of fact, a dedicated "child protection" page that encourages "safe surfing" is provided together with the aforementioned "family filter".

Main findings in relation to the website

Only marital status, username, email and date of birth are required to open an account on Dailymotion. However, users are free to add more personal information to their profile. By default, phone number, language, home address, zip code and email are always private and they cannot be made public by users even

if they wanted to. Private information is not made available to friends, other users or non-users. The last name and the date of birth can be made private if the user wishes to, but by default they are public. All the other information contained on a minor's profile is available to both users and non-registered users. By default, the public version of profiles of minors in Dailymotion contains the following personal information (if provided by the minor): username, full name, gender, age, city and country where the minor lives, online status, list of contacts, videos uploaded by the minor, favourites (videos selected as favourite by the minor), playlists created by the minor, comments made on the minor's profile and the date when the minor joined Dailymotion.

By default, only users who have uploaded videos to their profiles can be found in Dailymotion via the internal search engine. By typing the full name of users (including minors) or their usernames, their videos are retrieved. Videos contain the hyperlinked username of the user who uploaded the video. By clicking on this link direct access to the users' public profile is granted to registered and non-registered users. Users who haven't uploaded videos do not appear in name searches. By default, the internal search engine is set to find videos. However, if this option is set to find members, no minors are found, but a link to the videos found under the search name (including those of minors) is still provided. By clicking on this link users are directed to the videos found which, as previously mentioned, include the hyperlinked username which grants access to users' public profiles. Testing indicates that even though users younger than 18 are, indeed, excluded from members search, their profiles can still be found via the videos they upload. In other words, minors are excluded from members search, but are not excluded from other types of search, such as video search.

With default privacy settings, public profiles of minors and their videos can also be found via external search engines (e.g. Google). By default, all users may comment other users` videos. Users can also choose for each video if anyone can see the video, only friends, or only the user, using the button labelled "Edit infos" ("Modifier les informations"). In this "edit info" page, it is as well possible to choose if anyone can post comments or only people that can see the video. By default, only friends can post comments to the user profile, but it is also possible to disable this option so that no one can post comments on one`s profile. Private messages can only be sent by friends. Therefore, apart from friends' requests, minors cannot be contacted "privately" by any other user or non-user.

Users can easily delete any comment, either on a video or on the profile. However, there is no obvious way to report a comment with a button within the page. Users cannot chose to pre-moderate comments on their videos. Users may reject friends' requests or block other users. Users can also choose to receive useful notifications by email (e.g. when a comment is added to a video, when a new friend request is received, etc.).

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration states that Dailymotion provides abuse reporting mechanisms available to users at all times. For instance, abuse reporting buttons are placed beneath every uploaded video. Users can also contact the support team "at any time via the feedback page."

It is not clear from the self-declaration if the procedure to report inappropriate conduct or content is easily understandable for children (as well as for adults) or if it is age-appropriate. Nevertheless, it is mentioned that the reports are acted upon expeditiously, usually within 8 hours. The self-declaration does not include explicit information on if/how users are provided with the information they need to make an effective report. However it does mention that Dailymotion has developed an educational video for young people where they encourage them to report any inappropriate content they may come across.

Main findings in relation to the website

As stated in the self-declaration, inappropriate content can be easily reported at any time by using the report ("signaler") button at the bottom of any video. When clicking on the button, a simple report form appears where users can select the nature of the issue being reported (e.g. violence, porn, child pornography, etc.) and

they also have the possibility to add extra information about the situation being reported. Once the report is sent, the user is informed that the report has been transferred to the team.

During testing, a fictional gory video was reported to Dailymotion by means of the report button available under the video. A (fake) minor created for this test reported that she found the video scary and asked the provider for help. No further communication was received from Dailymotion in the following days. Even 15 days after having sent the report, the video was still available for minors on the site and the minor still had got no reply from the provider. Even though it can be argued that the content of the video reported was not really inappropriate (it was labelled as creative content), the minor asking for help never got a reply from the provider nor help on how to deal with potential inappropriate content found on the site.

Dailymotion offers a user-friendly mechanism to report inappropriate videos (via the "signaller" button placed next to every video). There is also a contact form where users can report other types of abuse, for instance inappropriate conduct or contact (e.g. harassment, sexual abuse, etc.). This online form was not so easily found on the website, but once identified; it was easy to use. Users also have the option to delete comments and/or block users.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Upon receipt of notification of alleged illegal content or conduct the service provider claims that they review and act upon all notifications from users "in a timely fashion, generally within 8 hours". The provider also claims to have mechanisms in place to review and process notifications from users including an automatic explicit content filtering system by means of which, suspicious videos tagged with keywords in the Dailymotion "blacklist" are sent to the support team for review.

The provider claims to liaise with French legal authorities to report dangerous behaviour identified either in the videos uploaded by users and/or in the comments associated to such videos. If needed, and in case of cybercrime, Dailymotion claims it will get in touch with the specialized French police bureau OCLCTIC.

Because of ethical reasons, Principle 5 was not tested on the website.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to Dailymotion, users of this SNS are provided with a range of privacy setting options that allow them to control their personal information and their interactions with other users. They can, among other things, hide any personal information provided during registration, they can reject friends 'requests, block other users, block commenting on their videos, etc.

According to Dailymotion, users are provided with exhaustive information on their privacy policy (accessible from a permanent link in the footer of the service) to help them make informed decisions about the information they post online. Besides, Dailymotion claims to provide educational videos for young people about surfing the Internet safely including specific privacy tips such as: do not share personal information or report any inappropriate content you may come across.

The service provider has taken into consideration the implications of automatically uploading information provided by users (during registration) onto their profiles by allowing users to decide if they want to hide any personal information provided by them during the registration process.

Main findings in relation to the website

As previously mentioned, only some pieces of information (e.g. last name and date of birth) can be made public or private at all times. The rest of the information contained in users` profiles is either always public (e.g. gender) or always private (e.g. telephone number). The profile page form makes clear to users which pieces of information are public and which are not. Regarding the videos posted on one's profile, users have the option to upload their videos as "private". This option can be chosen during the upload or at any time after publication. Any video set as "private" has a dedicated private URL shown under the player. This URL can be shared with anyone the user wishes to share their video with (including friends and non friends).

Users, including minors, can be "contacted" through several means: any registered user can post a comment on the video; any registered user can ask a minor to be "friends". However, only friends can post comments on the minor`s profile or send a private message. Therefore, apart from friends' requests, minors cannot be contacted "privately" by non-friends, only via public comments left on videos.

The use of privacy settings is simple and easy to understand, since there are the few possibilities listed above. Indeed, probably the main strength of the use of profiles on Dailymotion is its simplicity. Dailymotion is not a typical SNS but rather a platform centred on the sharing of videos themselves. As such, the only communication possibilities offered are commenting a video or a profile (if the user authorised it, see principle 3).

Deleting a profile is quite easy. In order to delete a profile, users have to go on the "personal info" ("informations personnelles") page and click on the "click here if you want to delete your account" link at the bottom of the page. This link is not very visible on the page, but the process is clearly explained in the FAQ page (fourth question of the FAQ). When clicking on the link, users are warned that they will lose everything (videos, favourites, groups, friends…) and that this is an irreversible process.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

Dailymotion assesses their service to identify potential risks to children and young people via automated mechanisms such as filtering tools to detect inappropriate content and via the reviewing of potential inappropriate or illegal content by the Dailymotion support team.

The provider claims that in order to support the compliance with the Terms of Service, technical tools (e.g. the aforementioned family filter) to flag potentially illegal or prohibited content and user-generated reports are in place. The filter sends alerts to the support team who reviews the suspicious content to make sure no inappropriate content is uploaded to the site.

Finally, the self-declaration indicates that "the support team reviews the videos to make sure there is no inappropriate content available on the site". According to the provider, the Support team "works 24/7 to review and act upon all notifications. All reports from users are handled in a timely fashion, generally within 8 hours".

Because of ethical reasons, principle 7 was not tested on the website.

Summary of Results and Conclusions

On the website, Principles 1, 3 and 6 were very satisfactorily assessed while Principles 2 and 4 were rather satisfactorily assessed regarding Dailymotion's commitment expressed in its self-declaration. Dailymotion offers clear, age-appropriate and easily accessible safety information targeted at children, parents and educators. Users` profiles do not contain much personal information. The profile management page clearly indicates whether every information field is public or private ("public data" or "private data"). As our tests

demonstrated, no highly inappropriate or illegal content (e.g. pornography or very violent content) was found on the site. On Dailymotion there is a "sexy" non-pornographic channel, but content labelled as "explicit" is not accessible to minors whose family filter is set to "on". Some areas of attention include:

- Although the site contains general safety information as well as safety information for children, the information specifically targeted at children on the site is rather limited.
- The available "family" filter that restricts access to potentially "inappropriate" content (e.g. the sexy channel) can be set to "off" by registered, signed-in minors if they modify their date of birth to a suitable one above 18 years old. Moreover, all non-registered users (including minors) can turn the family filter "off" without having to verify their age.
- Profiles of minors who have uploaded videos to their profiles can be searched by name via the internal and external search engines.
- Testing indicates that even though, as stated in the self-declaration, users younger than 18 are excluded from members search, their profiles can still be found via the videos they upload. In other words, minors are excluded from members search, but are not excluded from other types of search, such as video search.
- Even though a user-friendly reporting mechanism to report inappropriate content is available, the minor asking for help never got a reply from the provider nor help on how to deal with potential inappropriate content found on the site.
- No child-friendly reporting mechanism to report inappropriate conduct or contact is available on the site.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4		x	
5	x		
6		x	
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2		x	
3	x		
4		x	
6	x		

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
HABBO HOTEL

Dr. Jo Bryce, University of Central Lancashire, UK
Dr. Niina Uusitalo, University of Tampere, Finland
Dr. Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Habbo Hotel is a virtual world which provides a platform for social networking, gaming and community development for young people, with a general focus on users aged 13-18. In general, users below this age are not permitted to register on the service, except in a few countries like, for instance, Finland where the minimum age requirement is 10. Habbo was launched in 2000. It has customers in 150 countries. (e.g., UK, Belgium, Italy), and it is available in 11 languages (e.g., English, Portuguese, German, French). As of March 2011, the service had 210,000,000 registered users and over 11,000,000 unique visitors per month[1]. On the site users create a unique avatar, associated profile and their own personalised room. According to Sulake, there are currently over 120 million user-generated rooms in the different Habbo communities[2]. These and official rooms (virtual hotel's rooms, cafés, clubs, the pool area, etc.) are the focus of online interactions and community development. The profile pages can be customised with a guestbook, sticky notes and other widgets. Messages can also be sent between users by Minimail, through chat in different rooms, and by leaving stickies in chat rooms. Users can purchase credits for the virtual world which enable customization of avatars and purchase of other virtual products (e.g., furniture, clothes, pets). *Entering the site is free, but to access services users need to buy the virtual currency, Habbo Credits. Credits are used to pay for virtual furniture and homepage gadgets. Users can* play games, train pets, connect with friends, decorate their own rooms and Habbo homepages on the site and they can *s*wap virtual merchandise with other users.

The following is a report of the analysis of the self-declaration provided by Habbo Hotel and the testing of its website carried out in the period April-May, 2011. Habbo was tested in both the Finnish and the English (UK) versions of the site.

Summary of main findings

Habbo hotel has generally been successful in implementing the safety measures committed to in their self-declaration. In several sections of the site, the service provides accessible safety information for children and young people which is age appropriate as well as associated information for parents and carers (e.g. parents are encouraged to discuss safe internet use with their children). Although, the Terms of Service provided are framed in complex technical and legal language, the Habbo Way pages provide this information in more age appropriate language, including the types of behaviours which violate these terms and potential consequences.

The minimum age requirement of this SNS is 13 years old. In the Finnish version of the site parents of under 15-year-old users are informed of the child's registration to the site. There is no equivalent action in place for users under 15 in the English version. Inappropriate content was effectively restricted from the site. It was forbidden to enquire or give private information whilst using the virtual world. Users were not able to upload pictures, videos or their personal information on the site and the site also provides several filters to prevent certain types of disclosure and inappropriate content. In spite of the limited amount and type of personal information which users can post and share, tests demonstrated that widgets such as the guestbook, stickies and Minimail can be used to disclose such data. Besides, even though the use of filtering and monitoring tools

[1] Source: http://sulake.com/habbo/?navi=2; accessed 06.05.11
[2] http://www.sulake.com/press/releases/2011-01-20-Habbo_Hotel_Hits_200_Million_Registrations_.html

in the service work effectively, there are ways to circumvent these mechanisms (e.g., by describing phone numbers in words).

The SNS provides a variety of reporting mechanisms reflecting the different applications available, and these are prominent, accessible and easy to use. The user reports in both language versions of the site were acted on quickly. The service provides a number of privacy settings (e.g. removing, muting or blocking characters, restricting other users from seeing their profile page, rejecting friendship requests, etc.) which are also accessible and easy to use. However, they lack complexity and do not enable a distinction between general users and friends. Users are also unable to delete their account, and the suggested alternative may be seen as difficult or overly time consuming by young people.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

The service provider states that they offer *clear* guidance for children and young people on how to navigate their website safely. This is mainly done via the "house rules" (the Habbo way) which, according to the provider, deliver clear instructions for young children on what constitutes good and safe behaviour inside the community. The provider also states that the website provides safety tips and regular e-safety campaigns on the site and also externally via the Habbo infobus.

Habbo specifies in its self-declaration what constitutes inappropriate behaviour and the consequences thereof, for example, engaging in inappropriate discussions (e.g. of a sexual nature); exchanging personal information such as phone numbers; using certain forbidden words or terms, etc. Players who engage in inappropriate interactions can be muted. Other more explicit types of inappropriate behaviours and their consequences are detailed in the link to the "Habbo Way" provided in the self-declaration. These include: bullying is forbidden, or users who break the rules can be banned from the site. The self-declaration provides a link to the "Habbo Way" where information on the consequences of inappropriate behaviour is found. According to the provider, this information is easy-to-understand for young children and teenagers.

The signatory claims that all Habbo communities have local parental safety guidelines. A link to such guidelines containing a few general tips on how to monitor young children`s behaviour online is provided in the self-declaration. The self-declaration does not mention if Habbo hotel offers parents and/or teachers any technical controls on their website.

Main findings in relation to the website

The SNS provides clear and targeted Internet safety information for young people and parents. This information addresses general issues of online safety and safe use of the service and can be found in several sections of the site, namely on the "house rules", Frequently Asked Questions (FAQ) and Support. In the English version of the site, there are also links to other sources of information and support (e.g., charities, helplines, etc.). The safety information for young people and parents can be accessed in a number of different ways. There are direct links from the homepage of the service to information for both audiences which allow those not registered with the service to access related materials. There are a variety of ways in which young people can access information on safe use of the service and reporting problems when signed into the service (e.g., from the profile page, within chat rooms, and via message boards). The information contained in these pages is clear and accessible for the target audiences. In both language versions of the site the SNS provides a separate section for parents which provides specific information on how to use the service safely, as well as some general safety tips. In the English version some links to external agencies were also found. In none of the versions tested, there is information targeted at schools or teachers, though the information for parents would be equally accessible for these groups. Some safety guidance was also provided in visual form. In the "house rules" there were pictures of virtual characters who tackled safety risks (e.g. how to reply to someone

fishing for passwords). Inside the virtual world there was safety information on the homepage. Users could also use a "virtual robot" to answer questions on safety or other problems related to the use of the site.

The service provides Terms of Use for the general public which can be accessed from the bottom of the homepage (where links to the Privacy Policy, Safety Tips, etc. are also situated). The Terms of Use are not specifically targeted at children and young people, and the text is very technical / legal in places. This is particularly the case with the included descriptions of behaviours which constitute violations (e.g., 'ethnically or otherwise objectionable comments'). However, the main issues relating to inappropriate use of the service, and associated violations are described in more age-appropriate language within the Habbo Way pages. Although the service provider included information about what constitutes inappropriate behaviour on the site, for instance aggressive and violent behaviour, taking part in sexual actions and suggestions, and divulging personal information to other users, in the Finnish version of the site, the consequences of inappropriate behaviour are not described. The Terms and conditions only state that Sulake has the right to prevent users from using the service if rules are violated. On the contrary, the English version of the site gives concrete examples of what can happen in response to violations (e.g., moderator alerts, removal from public rooms or being banned).

The main strength of the SNS in relation to Principle 1 is the accessible and age appropriate nature of safety information for young people, particularly the Habbo Way Pages (these can also be accessed through the help menu when in the chat rooms). The main weakness is the technical and legal complexity of the language used to describe the Terms of Service.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

Sulake claims that they employ mechanisms to ensure the limited exposure to potentially inappropriate content and contact for children. The provider claims that users can`t upload any real photos or videos and sharing personal information such as contact details is forbidden. The self-declaration mentions that these potentially "inappropriate" or forbidden activities are monitored through automated tools such as special filters designed to support the moderation and monitor interaction on the site. Furthermore, Habbo hotel claims it does not host any "adult" content and does not have any specific sections for adults only.

According to the self-declaration, the minimum age requirement in order to subscribe to the website is 13 years old in most countries where the service operates, but it may vary depending on the location. The provider claims that users younger than the minimum age required are denied access. According to the signatory, depending on the country, some additional measures are taken by the provider in order to identify and delete under-age users from their services[3]. For instance, in some countries it is not possible to register from the same computer with a different age, while in other countries an e-mail is sent to parents informing them that their children have created an account on the site. The self-declaration does not mention if Habbo hotel offers parents and/or teachers any technical controls on their website.

Main findings in relation to the website

In the two language versions tested, the minimum age requirement is different: In the UK version it is 13 years old and in Finland it is 10 years old. This is clearly stated in the Terms of Service, Privacy Policy and information for parents. In the Finnish version of the site, users younger than 15 are obliged to provide their parents' e-mail address before registering so that their parents can be informed about their registration on the site. This e-mail is merely informative and does not ask parents for their permission for their child to use the site. There is no equivalent action in place for users under 15 in the English version. In both language versions tested, users are required to provide their date of birth when signing up, as well as their name, gender and a valid email address. Registration is denied if the provided information indicates that the user is aged below 13. However, as

[3] Only if their Terms require a minimum age

demonstrated by testing, there are no technical or legal mechanisms (at least in the UK and Finland) to prevent the user returning to the registration page and amending their age to be above the minimum required.

There were no functionalities on the site in order to label, rate or age restrict content or chat rooms for minors as there are no specific sections which include adult content. Confirming the analysis of the self-declaration, the site does not provide parental controls, but has its own set of filtering and monitoring tools which are used to block inappropriate content or chat.

The main strength of the SNS in relation to Principle 2 was that inappropriate content was effectively restricted from the site. The main weakness of the SNS in relation to Principle 2 is the lack of technical or other tools to prevent under aged users from amending their date of birth to register with the site.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

The provider claims to have in place a wide range of technical tools to support the community management and moderation particularly with regards to inappropriate or unwanted content or conduct. These include: the automatic saving of the chat log of the discussion; players who are engaged in inappropriate discussions (e.g. of sexual nature) are automatically muted and a filter prevents email addresses and phone numbers from easily being given out).

The self-declaration maintains that Habbo hotel is not a typical "social networking service" and even though, users do have profiles on the site, they are not allowed to share personal information such as contact details or upload pictures or videos to the site. The provider further claims that users can limit access to their profiles by preventing others from sending friends` requests or being followed inside Habbo. According to the provider, users also have the possibility to 'mute out' other players` chat from their private rooms temporarily or for longer periods.

As previously mentioned, the service provider claims it supports the safety education of parents in order to help them protect children and young people by means of parental guidelines. It is not explicitly mentioned if specific information on safety tools (e.g. filtering software) is given on the website.

Main findings in relation to the website

All users are searchable within the service but this is only successful if the username (not the real name) is known. This information could be determined by seeing another user in a chat room and searching their username, or if they publicly posted their Habbo username somewhere else online. It is also possible to search for Habbo's at random which could lead to publicly available profile pages, guestbook messages and friend requests. Users cannot be identified via external search engines even if their Habbo username is known. The profile pages of all users are set to public by default. In both language versions tested, profiles of minors can be potentially viewed by all users if their username is known (as described above), and through accessing friends-of-friends on their profile pages. The profile page, however, only contains the username and online status in default setting which limits the amount of personal information they contain. In both versions tested, the friends list is not included by default and must be added to the profile page by the user. Besides, it was forbidden to post personal information on the profile page (e.g. pictures, videos, etc.) and there is also a reminder of this rule on each profile page. Users, however, can share personal information by leaving sticky notes in other users' rooms (if publicly accessible), and on the Guestbook if it is voluntarily added to the profile page by the account holder). Stickies can also be attached to profile pages, and left in users' room if they have a noticeboard or sticky pole. Both comments and messages are not pre-moderated, but can be deleted or flagged as inappropriate. In the English version of the site, stickies must be purchased using credits, although credits can also be earned by quests and participating in surveys on the site. In the Finnish version users can post stickies on their own homepage without having to purchase any credits.

Users can be contacted by other people via friend requests, but not by non-users of the service. The service allows users to reject friend requests and choose not to receive friend requests at all; they can also delete

accepted friends, and ignore friends and other users in chat rooms. There is no ability to prevent users who are not friends from seeing the profile page unless the user makes it invisible to everyone (including friends) via the privacy settings.

User's friends can also send them messages using the Minimail application, which also provides the option to delete and report inappropriate messages. There are filtering and monitoring tools which block swearing, email and phone numbers in chat, Minimail, stickies and guestbooks. However, as tests demonstrated, sending phone numbers in words via Minimail, the guestbook or chat was possible[4]. There is also active monitoring of synchronous chatting on the site and a warning to this effect is included when users enter chat rooms. During testing an adult tried to get private information from a minor user in one of the virtual hotel rooms. The adult obtained some information (place of residence, school and address), but phone numbers or e-mail addresses were replaced by asterisks on the screen. When the minor tried to give a phone number for the second time, the moderator issued a warning on the adult's screen explaining that enquiring or giving phone numbers was forbidden according to the rules of the site. No warning was received when typing in words so phone number could eventually be communicated. During testing, the Finnish version of the site also provided a "nonsense filter" (Höpöfiltteri)[5] for users under the age of 13, which translated inappropriate terms to the word "nonsense" (höpö).

The strengths of this SNS in relation to Principle 3 are that the default settings make no personal information available on the profile page and that users were not able to upload pictures or videos on the site. In theory, users were not allowed to upload their personal information on the site, either. However, as tests demonstrated, personal information could be disclosed in chat rooms, on stickies and the guestbook. Even though the use of filtering and monitoring tools in the service work effectively, there are ways to circumvent these mechanisms (e.g., by describing phone numbers in words).

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration states that Habbo provides "easy ways to report content, suspicious behaviour or other issues taking place in the virtual community". According to the provider, the Reporting mechanism "Call for Help" button is located in the main toolset inside the world. Via this button users can get quick replies to the most common questions, but they can also report abuse to a moderator. Inappropriate content can also be reported to the moderation staff via the Habbo web (Habbo homepages, guest books, group discussion forums) and the customer support portal contains useful information for players and their parents. The self-declaration does not indicate if user reports are acknowledged or if they are acted upon expeditiously.

Main findings in relation to the website

The SNS provides a variety of easy-to-use mechanisms to report inappropriate conduct and contact from other users. Their exact operation depends on the specific type of application to which they are related. As stated in the self-declaration, the most prominent reporting mechanism was the Help-button found on every page of the virtual world. Through this link users could report inappropriate behaviour or bullying. The Help-button was age-appropriate, user-friendly and easily accessible. This 'call for help' mechanism, available in the user's own

[4] According to the provider, blocking numbers written in words would not be a feasible solution because by doing this other (written) content would be unnecessarily blocked as well.

[5] According to the provider, the "höpö" filter does no longer exist. Nowadays filtered words are replaced by asterisks (##) instead of by the word "höpö". The provider further claims that this filter is in place in all Habbo communities and that it is "on" by default for all users. Only children over 13 year olds can turn it off.

room and other chat rooms, allows users to select another user and 'ignore' or 'report' them. Selecting 'report' links to a list of potential problems (e.g., bullying, scamming) which the user selects. They are then asked to provide a brief description of the problem, and this is sent as a call for help to the moderators for investigation / action. The Help-link was available at all times inside the virtual world.

Inappropriate content / messages in Minimail or the guestbook can be flagged by selecting the red flag icon on each message. These reports are sent to the moderator and the user can remove the person who sent them the message. There is no clear reporting mechanism link from the homepage of the service, though once users have signed in there is a link to report abuse on their profile page and all other pages in the site. There is information in the Habbo Way and Report Abuse pages which provides users with the necessary information to make an effective report. There is also a help option within the rooms which allows access to similar details and a menu-based selection for reporting as described above. The reporting information for users specifies that all reports will be acknowledged and acted on as soon as possible (though no specific timescale is indicated). The process of using each of the different reporting mechanisms is described in the Habbo Way pages and the information accompanying each specific measure. This includes what happens to the report, how it is processed and how users or content reported is subsequently dealt with. For example, when flagging inappropriate content in Minimail, the associated information specifies that reports are sent to the moderator and the user can delete the person who sent them the message. Moderators can impose a variety of bans for users who have been found to have breached the Terms of Use. These also vary in length of time depending on the nature and severity of the behaviour. In the English version of the site, these different bans are described in the FAQ pages, and a message explaining the type of ban imposed is sent to users who have been found to have breached the Terms of Use in this way. In the Finnish version of the site the consequences of breaching Terms of Use are not specified. There is only a mention that Sulake can ban the users totally or partially if they break the rules.

During testing, two minors posted nasty comments on a "bullied" minor's guest list and on one of the "bullies" home page and guest list. In the Finnish version of the site, the bullied minor reported this problem to the moderators via the "Help" button. The report was acknowledged immediately and acted upon expeditiously. Indeed, the minor received a swift response to the query within one minute of leaving the report. The reported contents were not automatically removed. However, the bullied minor was guided further to flag the inappropriate contents on the "bullies" profile pages, which the bullied minor did. The bullied minor received an automatic response that the issue was being handled and the flagged contents were removed within 24 hours. In the English version of the site, when reporting an inappropriate message (bullying) left on the guestbook of a minor (created for this test), an automatic message was generated indicating that the report would be investigated by the moderators and action taken if necessary. Although there was no further contact with the minor who had made the report, the message was deleted. There was no contact or message to the user who had posted the message about their behaviour through Habbo or their external email.

The main strengths of the SNS in relation to Principle 4 are the variety of different reporting mechanisms for the different applications, their accessibility from within the service, and the speed of response in taking action against reports. The main weakness is that there is no link from the customer support query form to the reporting pages or mechanisms. Users on this form are told that they cannot use this facility to report abuse, but there is no direct link to the relevant sections of the site. This could be problematic for parents who want to report a problem relating to abusive or inappropriate behaviour and cannot log into the SNS.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

According to Sulake reports referring to illegal content and conduct are top priority and are handled urgently. Images, text or other content, which is illegal, are removed immediately upon notice and saved for possible police investigations. From the self-declaration it is not clear what happens with other types of inappropriate (but not illegal) content, for instance, bullying comments, pictures, videos, etc.

The service provider claims to have implemented arrangements to share reports of illegal content or conduct with the relevant law enforcement bodies and/or hotlines. Concretely speaking, Sulake claims it works hand-in-hand with local authorities and immediately reports illegal content or conduct to them.

Because of ethical reasons, Principle 5 was not tested on the site.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

The self-declaration states that users of this SNS are provided with a range of privacy setting options. For instance, Habbo users can limit access to their profiles, they can also prevent others from sending friends requests or from being followed inside Habbo; they can also choose if their profile and online status are public or not. According to the self-declaration, users are also provided with supporting information to help them make informed decisions about the information they post online especially with regards to the "importance of keeping personal information safe".

The self-declaration states that even though users do have profile pages (that allow them to present their "virtual identity""and publish other types of content) on the site, "users are anonymous, i.e. they are not allowed to share real-life content (such as images or videos) or personal information".

Main findings in relation to the website

The privacy settings are easy to use, and can be accessed by users at any time through the associated page in account settings in the profile pages. There is also a link through to these settings from within the chat rooms. The privacy settings available on this SNS relate to who has access to the profile page (nobody or everybody), friend requests (enabled / not enabled), ability to view online status (nobody or everybody), and the ability for other people to follow users between rooms (nobody or friends). Users can also specify privacy options for managing access to their own rooms (e.g., open to all, ring the bell, password protected). Supporting information is not included on the page containing these settings, but there is a general warning against disclosing personal information online and on the site in the Habbo Way pages, and similar information is included in the Privacy Policy. There is also a sticky on the profile page which reiterates the importance of being careful not to disclose personal information to other users. The privacy settings are very easy to use for all users. However, they are binary and do not distinguish between general users and friends. No personal information except name, gender, date of birth and email address is required during registration. These are not included in the user profile.

Users could select for their profile page to be private from all other users, restrict others from seeing their online status and prevent friendship requests. Privacy options did not allow users to customize privacy settings regarding specific groups of people or specific contents. In practice no personal information could be shared with other users, not even with friends. By default, in both versions, profile pages of 'strangers' can be accessed (unless they are set to private) by clicking on their Habbo when in a public room. Other users of the virtual hotel could be muted or blocked from entering the user's private rooms. During testing a minor muted out an adult's chat. The functionality was easy to use by clicking on the adults' speech bubble and then the button "Mute". Information on this functionality could be found through the "Help" button under the heading: "How to get rid of a bully/troublemaker". Once clicking the mute-button, the adult's chat messages were no longer visible on the minor's screen. One could also remove friends from private rooms. During testing the minor blocked an adult from her living room after which the adult could not return to that specific room. Removing and blocking characters was easy and the functionality could easily be used by clicking the unwanted character.

The service does not delete profiles on request. In the British version this information is included in the customer support pages, and users are advised to scramble their password, change their email address, remove their furniture from their rooms, delete their rooms and spend any outstanding credits before they

cease using their account. In the Finnish version of the site, there was no specific information on how to delete one's account. However, some information is found in the "how can I delete an old character?" section where users are advised to move their furniture to a new character and to stop using the old character because, as stated in the FAQ section, Habbo administration removes characters from the database that have not been used in over 12 months as part of routine service maintenance. In none of the versions tested, there is information about what happens to the users` information after ceasing use of their account or deletion.

The main strength of the SNS in relation to Principle 6 is that privacy settings are effective and easy to use. However, they lack complexity and do not enable users to distinguish between general users and friends. Users are also unable to delete their account, and the suggested alternative may be seen as difficult or overly time consuming by young people.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

According to the self-declaration, the SNS provider assesses their service to identify potential risks to children and young people by means of human moderation supported by automated (e.g. filters) tools. "Community management, moderation and player support functions are assessed regularly and a headquarter lead team constantly develops the procedures and ways of working". The provider claims that their online environment is closely moderated and monitored, but also that safety education is promoted on the site. These are the main types of procedures employed by the SNS provider in order to promote compliance with the Terms of Service, Acceptable Use Policy and/or House Rules (e.g. human and/or automated forms of moderation; technical tools (e.g. filters) to flag potentially illegal or prohibited content; user-generated reports, etc.

Habbo claims that where human moderators are employed, reasonable steps are taken to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people. According to the provider, experienced and trained adult moderators are in charge of monitoring Habbo environment and these moderators` backgrounds are checked when hired.

Because of ethical reasons, Principle 7 was not tested on the site.

Summary of Results and Conclusions

On the website, Principles 1, 2, 4 and 6 were very satisfactorily assessed. Principle 3 was rather satisfactorily assessed. The main strengths of this SNS are the safe approach towards sharing personal information and privacy and also the user-friendliness and effectiveness of the reporting mechanisms available on the site. Areas for further improvement include:

- In theory, users were not allowed to upload their personal information on the site. However, as tests demonstrated, personal information could be disclosed in chat rooms, on stickies and the guestbook.
- Even though the use of filtering and monitoring tools in the service work effectively, there are ways to circumvent these mechanisms (e.g., by describing phone numbers in words).
- Privacy settings are easy to use. However, they lack complexity and do not enable users to distinguish between general users and friends.
- It is not possible to delete a profile, although Habbo administration removes characters from the database that have not been used in over 12 months as part of routine service maintenance.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3		x	
4		x	
5	x		
6		x	
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3		x	
4	x		
6	x		

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
FLICKR

Dr. Jo Bryce, University of Central Lancashire, UK
Dr. Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Flickr is an online platform which allows users to post and share video and images. It was launched in 2004, and is available internationally in 10 languages including English, Chinese, German and French. In 2010 it was reported that Flickr was hosting more than 5 billion images[6], though no specific data on current numbers of registered users could be found. It has a wide demographic base of users including minors and has a minimum registration age of 13. The service offers free and pro accounts, and provides social networking and community building tools. It also enables the creation of personalised profile pages containing information about users, and allows the development of contact lists of users. It has a variety of privacy settings which can determine access to content, and provides extensive safety information to users, both adults and minors.

Summary of main findings

Flickr has been successful in implementing the principles and safety measures described in their self-declaration. The service provides accessible and age-appropriate safety information for children and young people. Although the Terms of Service provided are framed in legal language, the Community Guidelines and FAQs provide this information in age appropriate language, including the types of behaviours which violate these terms and potential consequences. The main strength of the SNS in relation to Principle 2 is the use of Yahoo! ID to check the age of users and ensure compliance with age requirements. A child below 13 cannot change their Yahoo! ID to place their date of birth above the minimum age requirement for Flickr. However, as no 100% reliable age-verification mechanism exists up to date, there is no way to prevent a determined user registering another Yahoo! ID with the appropriate age, and then using this to sign into the service. Young people cannot be identified by adults using internal searches. Access to the profiles of minors is only possible if adults are on the associated contact list or if they are friends-of-friends, though the photos of all users are visible in searches, and can be commented on by all registered users by default. The amount of personal information required in the profile page is minimal, and minors are able to use the associated settings to determine accessibility of those details. Clear and accessible information about the risks associated with disclosure of personal information on Flickr is provided in the Community Guidelines. The privacy settings are accessible and easy to use for young people, and provide the ability to distinguish between different groups of users in managing access to content, etc. The reporting mechanisms provided by the service are also accessible and easy to use. The use of filtering and monitoring tools in the service to prevent young people from accessing inappropriate pictures is effective, and the response to reports of incorrect labelling was dealt with promptly in a manner consistent with the Community Guidelines.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

The provider claims to provide prominent safety guidance (common to different services which share similar features) in "central locations on the Yahoo! Portal (and outside the Terms of service)" (e.g. the Yahoo! Help Central linked from the Help home page and in dedicated safety pages aimed at parents and children via Yahoo! Safety) including safety information specifically targeted at parents and carers (e.g. teachers), as well as

[6] Source: http://blog.flickr.net/en/2010/09/19/5000000000/ (accessed 16.05.11).

specific guidance for children and young users. The self-declaration also states that the Yahoo! Privacy Policy offers users specific information on topics such as privacy and "the posting of information and content on user generated services".

The provider states that the general Yahoo! Terms of Service establish the general conditions of use for all Yahoo! Services including Flickr. Here, the consequences of breaching the terms of service are specified. Additionally, according to the provider, the Community Guidelines "set out standards of behaviour for community-based services" which are supplemented with additional guidelines for Flickr explaining the do`s and don`ts for users. According to the provider, this information is not only easy to understand for children and young users, but is also easily available via the footer of every page on Flickr. Relevant links to this information are provided in the self-declaration.

According to the provider, "Flickr does not provide tools which allow parents to control their children`s accounts". However, Yahoo! claims to provide relevant information to parents about other tools outside Yahoo! (e.g. parental controls) which can be used to supplement the safety features provided by Yahoo!

Main findings in relation to the website

Flickr provides clear, accessible and targeted safety information for young people, adult users and parents in the Community Guidelines and FAQs. There is also a wide range of information available on Yahoo! Safely which can also be accessed from the homepage of Flickr. This is a general online safety resource which has sections for parents, young people, general tips and product specific safety guides. It covers general issues of online safety, as well as safe use of specific Yahoo! services including Flickr. The section of the site for young people contains information on a wide variety of topics (e.g., cyberbullying, sexting etc.), and an archive of relevant safety videos. This includes links to a number of external sources of information for young people, parents / carers and teachers. There is a direct link to Yahoo! Safely from the homepage of Flickr, as well as through the Community Guidelines which can also be accessed from the homepage. Users do not need to be registered with Flickr to access these sources of information, enabling potential users and parents to find out more about the service without being a member or prior to registering.

The Terms of Service for Flickr are generic to all Yahoo! products and services, and can be accessed from the bottom of the homepage (where links to the Privacy Policy, Report Abuse link etc. are located). These are presented in a standard legal format with text formatted in separate, generally short paragraphs. It is a generic document which is not specifically targeted at children and young people. The text is framed in legal terms, and the included descriptions of behaviours which constitute violations (e.g., 'ethnically or otherwise objectionable comments') may not be sufficiently clear to young people. However, the main issues relating to inappropriate use of the service and associated violations (e.g., bullying, hate speech, posting violent or sexual content) are described in accessible and age-appropriate language within the Community Guidelines and FAQs. The consequences of violating the Terms of Service are also clearly described in these pages and include deletion of images, moderation of accounts, warnings and account deletion. The main strength of the SNS in relation to Principle 1 is the accessible and age-appropriate nature of safety information for young people and parents.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

The self-declaration states that the minimum age required to subscribe to Flickr is 13 and that technical blocks are in place to prevent users younger than 13 from obtaining a Flickr account. "Where a young user is found to have lied about their age and breached Yahoo! Terms of service, customer care will delete their Flickr Account and associated Yahoo! ID." The self-declaration refers to a number of measures in place to protect young users from inappropriate content and contact. These include requiring users and content partners to tag their content as "safe", "moderate" or "restricted" (in line with Flickr guidelines) which correspond to the safe search settings "off", "moderate" and "on". As stated by the provider, this mechanism, would allow the restriction of user-

generated content to minors. The content provider also claims to have the safe search option "on" by default for all users and that "logged-in users who have a registered age of 13-17 years cannot turn safe search to "off". In other words, users registered as 13-17 years old cannot view content tagged as "restricted"". According to the self-declaration, users aged 13-17 can; however, change their settings to allow access to content tagged as "moderate". Moderate content includes nudity, but only in an artistic context. "Content more explicit than this is wrongly tagged and users are encouraged to report this to Flickr's customer care team".

Main findings in relation to the website

Flickr has a minimum age of 13 for users, though the evaluator could not identify any specific mention of this in the Community Guidelines[7].To sign into Flickr, users must have a valid Yahoo! ID account (or can use Facebook or Google). Signing up for a Yahoo! ID requires the user to provide their name, gender, country, postcode and date of birth. This process generates an email address, username and password which can be used to sign up for other Yahoo! services including Flickr. These details are checked during the Flickr registration process, and users aged below 13 are not permitted to access or use the site. A child below 13 cannot change their Yahoo! ID to place their date of birth above the minimum age requirement for Flickr. However, as no 100% reliable age-verification mechanism exists up to date, there are no technical mechanisms to prevent a child registering another Yahoo! ID with the appropriate age, and then using this to sign into Flickr.

The service does not provide parental controls, but uses a system of classifying and filtering content to ensure that minors are prevented from accessing inappropriate pictures or videos. Information about this labelling/filtering mechanism is included in the Community Guidelines and FAQs, as well as the Flickr Safety Guide. Yahoo! Safely also provides parents with general information on different tools for increasing the safety of their children online. Content is rated by users as 'safe', 'moderate' or 'restricted'. Minors by default are restricted to access only 'safe' content, though this setting can be changed to allow access to that which is labelled as 'moderate'. A series of image searches were conducted with safesearch enabled (default for minors) using terms which could expose minors to inappropriate content (e.g. sex, violence, nudity, drugs, gore, porn), but they generally did not lead to problematic photos. There were some nude images which would be classified as artistic, as well as some photos of drug paraphernalia (e.g. things for smoking marihuana), but no pictures of drug taking as such. Tests also confirmed that minors are able to change the safesearch setting to enable access to moderate content ("safesearch moderate") using the privacy settings, though they cannot be changed to allow access to restricted content. Changing the default setting to 'moderate' provided access to some "inappropriate" images, including an image of a man with his genitals on display. According to the self-declaration, 'moderate' content includes nudity, but only in an artistic context, which was clearly not the case of some of the content found on the site. However, the provider argues in its self-declaration that "content more explicit than this is wrongly tagged and users are encouraged to report this to Flickr's customer care team". During testing, one image which contained pornographic material within the photo on a computer screen was identified. This image was reported to Flickr's customer care team and was, indeed, reclassified as described in relation to Principle 4.

The main strength of the SNS in relation to Principle 2 is the use of Yahoo! ID) to ensure compliance with age requirements. However, as no fully reliable age verification mechanisms exists up to date, it is not possible to prevent users aged below 13 creating an additional Yahoo! ID with an amended date of birth to register with the site. A less positive aspect regarding Principle 2 is the fact that registered; logged-in, minors have the opportunity to change the safe search settings to enable access to content tagged as "moderate" which, as tests demonstrated, can be inappropriately tagged in some cases. Nevertheless, testing also demonstrated that when inappropriate content is reported, the provider efficiently deals with it so that it is no longer available for minors).

[7] This has changed since testing, and this information is now stated in the FAQ's.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

The provider claims to employ a number of tools and technologies to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct. These include, among others, that profiles of users 13-17 are not searchable and users may create an online identity or nickname and use it instead of their real name. As stated by the provider, "Flickr profiles are not full profiles" (only the e-mail address is necessary to create one), still profiles in Flickr are "public by default" because they are believed to constitute a low risk to minors. The provider claims that, if they wish, users can create a profile page where they can share more information about themselves and their interests. They can also share their web URL or blog link but this is not required. According to the provider, "a profile is not the main entry point to Flickr for a user, i.e.: a user would typically visit a photostream and, if he chooses to, could visit the profile also, if they wanted more information."

The self-declaration also states that all users can block, ignore or delete users from their contact lists, they can also reject invitations and they can control who can see specific elements of their profiles and apply specific access control to each of their pictures (e.g. users can prevent others from viewing or commenting on their photos). According to the provider, users can also organize their contacts into "friends", "family", or "friends and family", of just "contacts" (who do not have the special privileges that friends or family have).

Main findings in relation to the website

The profiles of users below the age of 18 are not searchable via external search engines or internally within Flickr, even if the username is known, as this is prevented by default. Minors are also unable to change the associated settings to make their profiles searchable. However, their images are included in photo searches unless disabled through the privacy settings. By default, the visible personal information in the profile page of minors contains the username, gender, relationship status, likes and dislikes, and photostream. Gender and relationship status are not required information, and users have the option to choose a 'prefer not to say option' in response to these questions. Adding likes and dislikes information is also optional. These options limit the amount of personal information contained in profiles, but there are options for all users to add more detail about themselves. There is no pre-moderation facility for comments before they are published, but they can be deleted by the user.

Access to the different types of information of minors varies according to whether the user is a registered user, a "friend of a friend" or a contact. All registered users are able to make comments on the publicly accessible photos of minors by default, though only contacts can add tags or people. Photos identified in searches can provide access to the username of minors, as well as their gender and relationship status, likes and dislikes, and their photostream. It also provides an opportunity to send them Flickr mail and update (friend) requests, though the age and the contacts list are not visible. Adult users can also access the profile page of younger users and the same information as previously described if they are "friends of friends". Contacts also have access to this information, as well as the birthday, the email address of the user if made available, and the contacts list. Younger users can build up contact lists of both adults and minors, though contacts can also be blocked and deleted. The main difference between friends of friends and other registered, but not "connected" users lies not in the type of personal information (from the minor) they can access, which is the same in both cases, but rather in the ways to get access to such information. A friend of friend is automatically granted access to this information while other registered, non-connected users, can only have access to such information via the photostream of the minor.

The strengths of this SNS in relation to Principle 3 are that young people cannot be identified by adults using external nor internal searches. Users can only find a minor's profile if they know their photos (via the photostream) or their ID or URL. As stated in the self-declaration profiles are not the primary entry point, rather the content is so the risk of a minor's profile being found like this is rather limited. Still, if the profile is found, minors could eventually be contacted by users beyond their approved list of contacts (e.g. via Flickr mail

or by commenting on their photos). It must be noted, though, that even if a profile is found, users have control over the accessibility of the personal details contained in their profile and mandatory data field is limited (e.g. the minor's age would not be revealed to users beyond their approved list of contacts).

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The provider claims to provide easily accessible mechanisms to report inappropriate content, contact or behaviour on their website via a links to a "report abuse" form on the "permanent and prominent" footer on every page on Flickr. Besides, the provider claims to have in place a prominent "flag this photo" link next to every image on Flickr. According to the provider, "the report abuse form is easy to understand by all users, including children". The provider also states that reports are acted upon expeditiously, typically within a time-frame of 48 hours, although complex cases may need more time to be resolved. According to the provider, users receive guidance on the information they need to provide with their report and/or on what they can do to resolve the matter themselves. Finally, when they send a report they receive an on-screen or e-mail notification.

Main findings in relation to the website

Flickr provides one central reporting mechanism, as well as different ways to block users. There is extensive information in the Community Guidelines, FAQs and Flickr Safety Guide about reporting abusive behaviour, contact or content. The reporting mechanisms and related information are accessible for minors and easy to use. Information is provided on what happens to reports, and how users or content reported is subsequently dealt with. Each page of the site contains a link to a Report Abuse page which provides users with a list of potential problems (e.g., content which violates Terms of Use, inappropriate behaviour in groups) which can be reported and investigated. Users making a report are asked to select a specific problem and this either auto-generates related advice (e.g., on blocking users), generates a reporting form for content, or asks them to provide a brief description of the problem if they are reporting another user's behaviour. This menu system was used to report a picture which contained sexually explicit material. This generated an automatic message stating that the report would be investigated by the moderators and action taken if necessary. It also explained that there would be no further contact from Flickr unless they required further information. The image was reflagged as restricted by Flickr within 24 hours and could not be accessed by minors, consistent with the timescale described in the self-declaration (48 hours). Individual pictures can also be flagged as inappropriate using the related icon included with each picture. This leads to a pop up window which specifies how the image has been tagged, the user's search settings, and provides the option to classify the image as incorrectly flagged. The Community Guidelines state that Flickr can delete content, moderate accounts, send warnings or ultimately delete accounts for users who have been found to violate the Terms of Service. The main strength of the SNS in relation to Principle 4 is the accessibility of the reporting mechanisms, their ease of use and the accessibility of supporting information.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Yahoo! states that they have expeditious mechanisms in place to process notifications from users about content or conduct which breaches their terms of service and that reports of abuse are resolved in a timely manner. The self-declaration also refers to the arrangements Yahoo! has in place with relevant law enforcement agencies in Europe that include the handling of urgent matters within hours and the passing on of suspected illegal content or reports (e.g. in cases of grooming of minors) to relevant bodies. The self-declaration further indicates that Yahoo! supports the local hotline [8] in charge of handling reports related to

[8] Yahoo! indicates that the local hotline in the UK is the Internet Watch Foundation and that Yahoo!'s membership status is confirmed on the IWF website at http://www.iwf.org.uk/members.

images of child sexual abuse and that it provides links to such organizations in its Help Central page and Yahoo! Safely.

Because of ethical reasons, Principle 5 was not tested on the site.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to the self-declaration, users of Flickr are provided with a range of privacy setting options as well as with supporting information to help them make informed decisions about the information they post online via a permanent "Your Privacy" link at the foot of every page on Flickr. These settings can also be accessed by clicking on the username in the header of the page. Yahoo! claims to offer users a dedicated Privacy Centre with practical tips to manage user`s privacy and personal information. The provider also claims that "it is clear to users when completing their profile what content will be public".

Main findings in relation to the website

The privacy settings for Flickr are clearly available at all times through the account settings menu which is available under the 'you' tab on all pages. The settings enable users to control who has access to the profile page, contact lists, comments on photos, tags, etc. There are also options to change the privacy settings for individual photos and user blocking mechanisms which are accessible and easy to use for younger users. Supporting information is included on the specific page containing the privacy settings, and guidance about disclosing personal information on the site can also be found in the Community Guidelines, FAQs and Flickr Safety Guide. Default settings are provided by the service to prevent adults searching for the profiles of minors if they are not already contacts or friends of friends. The settings provide distinctions between contacts, friends and family, and can be used to allow or restrict access to certain activities (e.g., tagging, commenting on photos, etc.) for different users. Privacy settings also include the ability to block other users and contacts. This prevents access to the photostream or profile of the user who has blocked them, and use of the internal search function to locate them. The blocked user is also invisible to the person who instigated the block on the contact list of common friends. They do not receive a notification that this has occurred or an explanation why a contact / friend has disappeared from their contact list. Minors are able to use the search facility to find adults and contact them if they know the relevant username. They are then able to access the associated profile (if public) with full name, gender, relationship status (the associated default is also public). They can also access the profiles of users on the related contact list including other minors, and access any associated information included by default (e.g., gender, relationship status, likes and dislikes). The personal information required during registration is not automatically mapped onto the user profile. Other types of information can be added to the profile, but it is made clear that this information is not required by the service. Users are warned about disclosure of personal information and associated risks in the Community Guideline, FAQs and the Flickr Safety Guide. It is easy to delete an account on this service, and the associated information in the Account Settings makes it clear that all photos, videos and associated metadata is removed. The privacy settings are accessible and easy to use. They provide the ability to distinguish between different groups of users, and manage access to content and ability to engage in different activities accordingly.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

The provider claims to assess their service to identify potential risks to children and young people via report abuse forms generated and by the flagging of inappropriate photos by users. According to the provider, customer care agents typically handle complaints about content or conduct which breaches the Terms of service. Besides, the self-declaration states that "serious abuse in a Yahoo! Service may be escalated internally to a dedicated team within the Legal group which provides professional support and advice on more complex matters and determines an appropriate response".

The provider claims that the so-called community managers "engage with the community to promulgate and encourage respect for the standards of behavior set out in the community guidelines and the Yahoo! Terms of service". These community managers also offer help to users via the Help Forum.

Because of ethical reasons, Principle 7 was not tested on the site.

Summary of Results and Conclusions

On the website, all the principles were assessed as very satisfactorily implemented (See Table 2). The main strengths of this SNS are the availability of targeted safety information for minors and carers as well as the user-friendliness and effectiveness of the reporting mechanisms available on the site. The privacy settings are also accessible and easy to use and they provide the possibility for users to manage access to their personal content and the ability to engage in different activities accordingly. Some areas of attention include:

- Registered, logged-in, minors can change the safe search settings to enable access to "moderate" content which, as tests demonstrated, can be inappropriately tagged in some cases, thus potentially allowing access to some type of inappropriate content. Nevertheless, testing also demonstrated that when inappropriate content is reported, the provider efficiently deals with it so that it is no longer available for minors).

- As stated in the self-declaration profiles are not the primary entry point, rather the content is so the risk of a minor's profile being found is rather limited. Still, if the profile is found, minors could eventually be contacted by users beyond their approved list of contacts (e.g. via Flickr mail or by commenting on their photos). It must be noted, though, that even if a profile is found, users have control over the accessibility of the personal details contained in their profile and mandatory data field is limited (e.g. the minor's age would not be revealed to users beyond their approved list of contacts).

- "Friends of friends" and adults who identify minors through public photo searches have access to considerable personal information from younger users, namely, the username, gender, relationship status, likes and dislikes, and contacts list. Even though this information is not required by the service, if users choose to include it on their profiles, it becomes visible to friends of friends.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
5	x		
6	x		
7	x		

Table 1. Assessment of the Principles in the self-declaration

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
6	x		

Table 2. Implementation of the self-declaration on the website

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
YAHOO! PULSE

Dr. Jo Bryce, University of Central Lancashire, UK
Dr. Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Yahoo! Pulse is an online social networking platform which allows users to create a personalised profile, communicate with others, post videos and images, and provide updates to contacts. It was launched in 2010 to replace Yahoo! Profiles[9], though the photos, guestbook and blog applications are being disabled after May 2011[10]. It is difficult to find information on the number of Yahoo Pulse! users or available languages, but Yahoo! is available internationally in over 40 countries and languages (e.g., English, Chinese, Danish, Italian). Pulse has a minimum registration age of 13 but caters to a wide user demographic, and requires a Yahoo! ID to sign in. It provides a variety of privacy settings which control access to content, and provides extensive safety information to young and adult users.

Summary of main findings

Pulse has been successful in implementing the principles and safety measures described in their self-declaration. The service provides accessible and age-appropriate safety information for children and young people. Although the Terms of Service provided are framed in legal language, the Community Guidelines provide this information in age appropriate language, including behaviours which constitute violations and potential consequences. Yahoo! ID is used to ensure compliance with age requirements, although as no 100% reliable age-verification mechanism exists up to date, there are no specific technical or other tools to prevent users aged below 13 creating an additional ID with an amended date of birth to register with the site. Pulse provides young people with a high level of control over the amount of personal information included in their profile page through the accessible and easy to use Privacy Settings. It also provides clear and accessible information about the risks associated with disclosure of personal information on Pulse in the Community Guidelines and associated safety guidance. The reporting mechanisms provided by the service are also accessible and easy to use. The speed and nature of action taken in response to the test report was consistent with the timescale described in the self-declaration, and the nature of the violation and expected responses were made clear in the resulting email.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

The provider claims to provide prominent safety guidance (common to different services which share similar features) on the general Yahoo! Portal (e.g. the Yahoo! Help Central linked from the Help home page) including safety information specifically targeted at parents and carers (e.g. teachers) as well as specific guidance for children and young users. The self-declaration also states that the Yahoo! Privacy Policy offers users specific information on topics such as privacy and disclosing personal information and content on user generated services.

[9] Source: http://help.yahoo.com/l/uk/yahoo/pulse/welcome/welcome-01.html;_ylt=Apj14HgnfT40uLbQvKPfwMmLgHlG (Accessed 08.06.11).
[10] Source: http://pulse.yahoo.com/y/download_tool (Accessed 08.06.11).

The provider states that a Yahoo! ID is required in order to create a Yahoo! Pulse profile. When acquiring such an ID, users commit to general terms of service governing the use of all Yahoo! including Yahoo! Pulse. According to the provider, additional Community Guidelines "set out standards of behaviour for community-based services" which are supplemented with additional guidelines for Yahoo! Pulse explaining the do`s and don`ts for users and the possible consequences of breaching these guidelines. According to the provider, this information is not only easy to understand for children and young users, but is also easily available via the footer of every page on Yahoo! Pulse. Relevant links to this information are provided in the self-declaration.

Main findings in relation to the website

Pulse provides clear, accessible and targeted safety information for young people, adult users and parents in the Community Guidelines and the Pulse Safety Guide. There is also a wide range of information available on Yahoo! Safely which can also be accessed from the homepage of Pulse. This is a general online safety resource which has sections for parents, young people, general tips and product specific safety guides. It covers general issues of online safety, as well as safe use of specific Yahoo! services including Pulse. The section of the site for young people contains information on a wide variety of topics (e.g., cyberbullying, sexting, etc.), and an archive of relevant safety videos. This includes links to a number of external sources of information for young people, parents / carers and teachers. There is a direct link to Yahoo! Safely from the homepage of Pulse, as well as through the Community Guidelines which can also be accessed from the homepage. Users do not need to be registered with Pulse to access these sources of information, enabling potential users and parents to find out more about the service without being a member.

The Terms of Service for Pulse are generic to all Yahoo! products and services, and can be accessed from the bottom of the homepage (where links to the Privacy Policy, etc. are located). These are presented in a standard legal format with text formatted in separate, generally short paragraphs. It is a generic document which is not specifically targeted at children and young people, and the text is framed in legal terms which may not be sufficiently clear to them. However, the main issues relating to inappropriate use of the service and associated violations (e.g., bullying, hate speech, impersonation, violent or sexual content) are described in accessible and age-appropriate language within the Community Guidelines. The consequences of violating the Terms of Service are also clearly described in these pages and include the removal of abusive content, termination of the Yahoo! ID and access to all associated accounts. The main strength of the SNS in relation to Principle 1 is the accessible and age-appropriate nature of safety information for young people and parents.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

According to the self-declaration, the minimum age required to subscribe to Yahoo! Pulse is 13. The provider claims to have technical blocks in place to prevent users younger than 13 from creating a Yahoo! Pulse profile. "Where a young user is found to have lied about their age and breached Yahoo! Terms of service, customer care will delete their profile." The provider claims to have a number of measures in place to protect young users from inappropriate content and contact. These include: By default, users with a registered age of 13-17 years, can only share their profile information with their connections, although, if they wish, they can choose to share their profile with all users. The provider also claims to provide users with further advice on what content is or is not acceptable on the service via the Yahoo! Pulse help pages.

As stated in the self-declaration, "Yahoo! Pulse does not provide tools which allow parents to control their children`s accounts". However, they claim to provide relevant information to parents about other tools outside Yahoo! (e.g. parental controls) which can be used to supplement the safety features provided by Yahoo!

Main findings in relation to the website

Pulse has a minimum age of 13 for users. This is specified in the Community Guidelines, though not in the UK Terms of Service. Attempting to sign up as a minor aged below 13 for an ID resulted in a direction to set up

such an account. Users must have a valid Yahoo! ID account to sign into Pulse. Signing up for a Yahoo! ID requires the user to provide their name, gender, country, postcode and date of birth. This process generates an email address, username and password which can be used to register or sign into other Yahoo! services including Pulse. These details are checked when a user signs into Pulse for the first time, and users aged below 13 are not permitted access. However, there is no technical mechanism which can prevent a child registering another Yahoo! ID with the appropriate age, and using this to sign into Pulse.

There are no specific services or content designated as inappropriate for minors, and the testing did not identify content or postings of this nature, though the Community Guidelines asks that younger users be considered when using the service. As stated in the self-declaration, Pulse does not provide parental controls, but general information about parental monitoring and associated tools are included in Yahoo! Safely.

The main strength of the SNS in relation to Principle 2 is the use of Yahoo! ID to ensure compliance with age requirements, although as no 100% reliable age-verification mechanism exists up to date, there are no specific technical or other tools to prevent users aged below 13 creating an additional ID with an amended date of birth to register with the site. There is also no mention of age restrictions in the UK Terms of Service.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

The provider claims to employ a number of tools and technologies to assist children and young people in managing their experience on the service, particularly with regards to inappropriate or unwanted content or conduct. These include, among others, that users may create an online identity or nickname and use it instead of their real name; the profiles of 13-17 years old are, by default, shown to connections only so that even though all user profiles are searchable in Yahoo! Pulse, the *default* profiles of users aged 13-17 will not be shown; sharing contact information such as the user`s Messenger ID or email address is optional. If users select this option, it is, by default, set to “connections only”.

The self-declaration also states that all users can block, ignore or delete users from their contact lists, they can also accept or reject invitations to connect with other Yahoo! Pulse users, and they can control who can see specific elements of their profiles and apply specific access control to content posted by them (e.g. they can prevent other users from leaving comments in their guestbook, updates, blog or pictures by blocking them; they can also delete other users` comments left, etc.)

Main findings in relation to the website

The profiles of users below the age of 18 are not searchable via external search engines. Indeed, testing the internal search function did not enable the identification of adults or minors by first or full name. It is possible to make random internal searches in Pulse, but these did not enable access to the profile pages of users aged 13-17 by default.

The profile page contains the full name, username, gender and birthday of the user. Information about likes and dislikes can be included in the profile, but is only visible to contacts by default. Registered adult users who are not contacts of minors can access their profiles if they have friends who have young people on their contact list. These “friends of friends” are able to see minors’ username and gender, access and comment on their user updates (which are public by default), and send an update (friend) request. Adult “friends of friends” cannot see other personal information (e.g., likes / dislikes), photos or associated comments unless these are set to be publicly accessible. They cannot see the contact list, though this can be accessed by “friends of friends” who are minors.

Users are provided with privacy options when uploading photos, and by default this only allows contacts to have access and comment, though this can be changed to make them available to all users. All registered users are able to make comments on the publicly accessible updates of minors, but only contacts can access the guestbook or comment on photos by default. There is no pre-moderation facility for comments before they are

published, but they can be deleted or reported as inappropriate by the user. There are no private messages facilities on Yahoo! Pulse.

The strengths of this SNS in relation to Principle 3 are the minimal amount of personal information required in the profile page, and the high level of control that younger users have for determining its accessibility. There is also clear and accessible information about the risks associated with sharing personal details in the Community Guidelines and associated safety guidance.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The provider claims to provide easily accessible mechanisms to report inappropriate content, contact or behaviour on their website via a permanent link to a "report abuse" form on every profile page. Besides, the provider claims to have in place a prominent "report abuse" link next to every photo, blog entry, update and comment. Via this link users can report "anything that may breach the terms of service or require review by Yahoo! Pulse staff". According to the provider, the report abuse form is user-friendly even for children. The provider also states that reports are acted upon expeditiously, typically within a time-frame of 48 hours, although complex cases may need more time to be resolved. According to the provider, users receive guidance on the information they need to provide with their report and/or on what they can do to resolve the matter themselves, and whenever they send a report they receive an on-screen notification.

Main findings in relation to the website

There is extensive information in the Community Guidelines and Pulse Safety Guide about reporting abusive behaviour, contact or content. Pulse does not provide a link to its reporting mechanism at the bottom of each page (where links to the Terms of Service and safety information are located). Instead, individual Report Abuse links are provided on profiles, photos, updates and comments. These links direct the user to a menu-based reporting system, which differs slightly in terms of the information required depending on which part of the service is involved. The Report Abuse page asks users to select the particular problem they are reporting from a list (e.g., violations of Terms of Service, threats or violent content, harassment, etc.). The user is also asked to provide a brief description of the issue being reported. If the report is a profile or photo, the associated URL is also captured and included on the reporting form. The reporting page also includes a link to remove the connection with the specific user, as well as links to the Terms of Service and Community Guidelines in some instances. Users can also be blocked via the profile pages. Information about the action taken in response to violations of the Terms of Service is included in the Community Guidelines (e.g., remove abusive content, termination of the Yahoo! ID and all associated accounts). The reporting mechanisms and related information are accessible for minors and easy to use.

The reporting system was used to report bullying comments and photos posted to a minor by other young users. This generated an automatic message that acknowledged the submission of the report, and stated that it would be investigated and further action taken if necessary. Within 12 hours the minor making the report had received an email summarising the category of violation reported, a further link to the Terms of Service, and stated that the report would be investigated. There was no indication of the timescale for this, or whether they would hear anything further from Pulse, and they were not subsequently informed of the action taken by Yahoo! in response to the report. Approximately an hour after this email was sent; the user who had been reported received an email from Yahoo! reminding them of the Terms of Service and behaviours which constituted violations. They were informed that Yahoo! felt that these had been violated by the user, and that they should cease any related activity immediately. The comments and photos were not automatically removed by Pulse, but the user who had been reported was clearly informed that they should immediately delete content or activity from any parts of the account that were involved in the violation. This is consistent with the information provided in the self-declaration. However, they did not subsequently remove the bullying comments or pictures, and did not receive any further warnings as a result. The main strength of the SNS in relation to Principle 4 is the accessibility of the reporting mechanisms and their ease of use. The speed and

nature of action taken in response to the test report was consistent with the timescale described in the self-declaration, and the nature of the violation and expected responses were made clear in the resulting email.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Yahoo! states that they have expeditious mechanisms in place to process notifications from users about content or conduct which breaches their terms of service and that reports of abuse are resolved in a timely manner. Yahoo! claims to have arrangements in place with relevant law enforcement agencies in Europe that include the handling of urgent matters within hours and the passing on of suspected illegal content or reports (e.g. in cases of grooming of minors) to relevant bodies. The self-declaration further indicates that Yahoo! supports the local hotline[11] in charge of handling reports related to images of child sexual abuse and that it provides links to such organizations in its Help Central page and Yahoo! Safely[12].

Because of ethical reasons, Principle 5 was not tested on the site.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to the self-declaration, users of Yahoo! Pulse are provided with a range of easily-accessible and always available privacy setting options as well as with supporting information to help them make informed decisions about the information they post online via the "Settings" link at the top of every page on Yahoo! Pulse. Yahoo! also claims to offer users a dedicated Privacy Centre (accessible from the "privacy Policy" link at the foot of every page) with practical tips to manage user`s privacy and personal information. According to the provider, when completing their profile, users are clearly informed about what content will be made public. The self-declaration mentions that users can delete their Yahoo! Pulse account, but in order to do this, they must cancel their Yahoo! account.

Main findings in relation to the website

The privacy settings for Pulse are clearly available at all times through the settings tab which is present on all pages. These enable users to control who has access to the profile page, included personal information, updates, photos and comments. All the privacy settings are accessible and easy to use for younger users. Supporting information is included on the specific page containing the privacy settings, in the Privacy Policy, the Community Guidelines and the Pulse Safety Guide. The privacy settings provide distinctions between all users (everybody), contacts and nobody, and allow or restrict access to content and activities (e.g., guestbook, photos or comments). Privacy settings also include the ability to block other users and contacts.

No personal information is required in the registration process as the Yahoo! ID is used to sign into Pulse. Other types of information can be added to the profile, but is not required by the service. Users are warned about disclosure of personal information and associated risks in the Community Guideline and the Pulse Safety Guide. As stated in the self-declaration, it is not possible to delete a profile from Pulse unless the main Yahoo! ID account is terminated, though the privacy settings can be used to hide the profile from all other users. It is easy to find the associated information and settings. The strengths of this SNS in relation to Principle 6 are the accessibility and ease of use of the privacy settings. They provide the ability to distinguish between contacts and all users, and manage access to content and the ability to engage in different activities accordingly.

[11] Yahoo! indicates that the local hotline in the UK is the Internet Watch Foundation. Yahoo!'s membership status is confirmed on the IWF website at http://www.iwf.org.uk/members .

[12] Links to these bodies are available on Yahoo! Help Central http://help.yahoo.com/l/uk/yahoo/abuse/issues/report_other.html

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

The provider claims to assess their service to identify potential risks to children and young people via report abuse forms generated and by the flagging of inappropriate photos by users. According to the provider, customer care agents typically handle complaints about content or conduct which breaches the Terms of service. Besides, the self-declaration states that "serious abuse in a Yahoo! Service may be escalated internally to a dedicated team within the Legal group which provides professional support and advice on more complex matters and determines an appropriate response".

The provider claims that the so-called community managers "engage with the community to promulgate and encourage respect for the standards of behavior set out in the community guidelines and the Yahoo! Terms of service". These community managers also offer help to users via the Help Forum.

Because of ethical reasons, Principle 7 was not tested on the site.

Summary of Results and Conclusions

Principles 1, 2, 4 and 6 were very satisfactorily assessed and principle 3 was rather satisfactorily assessed. Yahoo! Pulse has been successful in implementing the principles and safety measures described in their self-declaration. The service provides accessible and age-appropriate safety information for children and young people***, while the Community Guidelines provide this information in a child-friendly format and language.*** Yahoo! ID is used to ensure compliance with age requirements. Yahoo! Pulse provides young people with a high level of control over the amount of personal information included in their profile page through the accessible and easy to use Privacy Settings. It also provides clear and accessible information about the risks associated with disclosure of personal information. The reporting mechanisms provided by the service are also accessible and easy to use. The speed and nature of action taken in response to the test report was consistent with the timescale described in the self-declaration, and the nature of the violation and expected responses were made clear in the resulting email. The testing on the website revealed some areas of attention, for instance:

- In spite that the self-declaration states that "profiles of users 13-17 years are defaulted to "connections only", testing demonstrated that registered adult users who are not contacts of minors can access their profiles if they have friends who have young people on their contact list. These "friends of friends" are able to see minors' username and gender, access and comment on their user updates (which are public by default), and send an update (friend) request. Adult "friends of friends" cannot see other personal information (e.g., likes / dislikes), photos and associated comments (on photos) unless these are set to be publicly accessible. They cannot see the contact list, though this can be accessed by "friends of friends" who are minors.

- The reporting mechanism proved user-friendly and quite effective, but the bullying pictures uploaded during testing were not removed from the site and the bullies did not get any further warnings for not having removed them.

- The fact that users cannot delete their Yahoo! Pulse profile unless their Yahoo! account is deleted may prevent users from deleting their accounts (even if they wished so) because by cancelling the Yahoo! account, users would also be unable to access / use any of the other Yahoo! services which use the associated username and password. However, Pulse provides the possibility for the users to hide their profile as an alternative[13].

[13] The information is available via the "Manage privacy settings" option on this page http://pulse.yahoo.com/y/settings. This is accessed via the "Settings" tab at the head of the Y! Pulse home page http://pulse.yahoo.com/.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
5	x		
6	x		
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3		x	
4	x		
6	x		

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
SKYROCK

Cédric Fluckiger, University of Lille 3, France
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Skyrock is a French speaking blogging platform, initiated by a popular French radio. It is specifically dedicated to teenagers. It exists mainly in French, but also in English, German, Italian, Spanish, Dutch and Portuguese. It was launched in 2002. According to Skyrock Website, it holds nearly 25 million profiles (on April 04 2011). The minimum age to register on this platform is 12. Here users can create profiles and blogs. On blogs, users can post articles, usually consisting of a picture and a short text. Skyrock is primarily based on the sharing of blogs with friends rather than on the use of and the sharing of applications such as quizzes, games, etc.

Summary of main findings

In Skyrock the safety information available for children, parents and educators is comprehensive, easy-to-understand and accessible. The reporting mechanism is easy to find and to use. Privacy settings are limited, but they are accessible and easy to use. Any user can set his/her blog to "secret", but the "profile" cannot be made fully private.

Other features of Skyrock include: adults who are not befriended with a minor (including "friends of friends") cannot invite him/her to a private discussion. On chat rooms, a visible message warning users to never communicate personal or contact information is displayed.

Some of the main strengths of the site are the availability and the quality of safety educational materials and the reporting mechanism, which proved to be easy to use, extremely rapid and efficient. One of the main weaknesses of the service provider is that, despite what is stated in the self-declaration, no mechanism to prevent the re-registration of under aged users (e.g. cookies) was found.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

Skyrock claims to provide clear, targeted guidance to minors and parents on how to navigate the website safely "*in a prominent, accesible and easy to understand format*". It also claims to provide education and tips about online safety and privacy in a clear, relevant and age-appropriate language throughout the site. These materials include, for instance, the anti-bullying campaign developed by INSAFE. The self-declaration also mentions that all users receive contextual security warnings whenever they are about to post content on the platform.

In relation to the Terms of use, the self-declaration states that before accepting the terms, users are offered a short, child-friendly summary of the "users' major engagements" with the site, but no concrete references were in the self-declaration regarding the consequences of inappropriate behaviour on the site.

Main findings in relation to the website

Confirming what is stated in the self-declaration, Skyrock provides very clear and comprehensive educational materials, targeted to children, parents and educators. It gives advice on topics such as privacy and reputation e.g. "*never give out personal information*", "*never publish anything that could later embarrass you*"); how to

deal with inappropriate content, etc. Simple warnings and ways of dealing with many problems are explained to children and children are encouraged to talk to adults or contact Skyrock if they encounter any problem. This information is accessible through the "safety" ("sécurité") link at the footer of the page. On the "parents" page, there are several links to organisations promoting a safer Internet (such as Insafe, e-enfance, Internet Sans Crainte, etc.).

Inappropriate behaviours are explained in the safety page using clear and non technical terms. The consequences of breaching the rules governing the site are explicitly developed in the general Terms of Use, however these are explained using rather technical and legal jargon while no concrete examples are given. Thus, the consequences of breaching the rules may be somehow difficult to understand for Children.

In both the parents and children safety page, children are explicitly warned that the information they post online may be spread worldwide and that it may even be used several years later.

Users may also access the "terms and conditions" ("conditions generales d'utilisation") page from the footer and from the "safety" page. A simplified Terms of Use version is easily accessible from the page especially targeted at children, and is easy to understand by children. All the information is in an adapted to children and complete textual format. Skyrock does not provide any videos or other formats to illustrate safety messages or the terms of use.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

The minimum age requirement to create an account on Skyrock is 12 years old. Skyrock claims to use a filtering algorithm to seek and delete individuals misrepresenting their age. According to Skyrock, the age registered by the user will determine which categories of age groups the user will be able to contact or be contacted by. As stated in the self-declaration, *"Skyrock employs cookies sessions, permanent cookies, email and IP addresses on its registration page to flag users who will change their age if the initial age was below the one specified in terms of Use"*. The provider also claims that their staff "actively searches out underage users manually. Upon discovery that a user is not 12 years or older, Skyrock.com deletes the user's account, blog and profile." Furthermore, a filtering algorithm that seeks and deletes users misrepresenting their age is in place.

Skyrock further declares that the service does not host any "adult" content and that it does not have any specific sections for adults only. Besides, the provider states that they use a filtering algorithm to forbid certain words, expressions and URLs considered as inappropriate. Apart from this, Skyrock claims to only display safe advertising banners and "family safe Google Ads".

Main findings in relation to the website

As stated in the self-declaration, the minimum age to register is 12. Children may access any page from Skyrock, as no part of this SNS is unsuitable for children. There are no sections or content labelled as "adult-only" on Skyrock. Regarding commercial content, there is an advert on every blog. Throughout the testing, no advert that could be considered as "unsafe" or "unsuitable for children" was found (e.g. adverts for Internet Explorer, Skyrock Videos, a commercial social network).

As our tests demonstrated, when a 9-year old child tried to register on Skyrock registration was denied. This was made explicit to the user by displaying the following message: *"You must be 12 years or over to sign up to Skyrock!"* and by taking the user back to a form where the age field was highlighted to be filled in. By providing a 12+ age on the age field it was possible for the 9-year old (created for this test) to successfully register on the site. Our tests (with Mozilla Firefox 3.6.16), therefore, suggest some deficiencies in the flagging system and the active manual searching of underage users referred to in the self-declaration as these mechanisms proved not

to be effective enough in identifying and deleting an underage user from their service[14], at least during the period that the testing lasted.

In Skyrock, there are no parental control tools available. However, children are encouraged (through the "safety" page) to talk about their blog with their parents, while clear and comprehensive safety information is given to parents to accompany their children on Skyrock.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

Skyrock employs several tools and technologies in order to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct. For instance, users can choose with whom to interact (although Skyrock limits the interaction between users who do not belong to the same age group). According to the provider, users can also manage posts and comments, as well as who post them, in their profile; they can also block other users, and prevent their images from being forwarded to other sites.

Skyrock also maintains that various tools are employed *"to identify anomalies in how a user might be using Skyrock.com. Users` behaviours are then rated and users can be excluded from the website*." Skyrock claims that user reporting is also used as a mechanism to flag illegal content or behaviour.

The self-declaration indicates that users under the age of 16 are unsearchable on search engines. Nothing is mentioned about 17-18 year olds, though. Still, it is not clear from the self-declaration if profiles of minors are set to "private" (by default).

Main findings in relation to the website

On Skyrock, any user has both a profile and a blog. On the profile, the information available to others depends on the fields filled in by the user. It may include nickname, age, gender, country and place of residence, hobbies, list of contacts, pictures, etc. All this information is visible to other users (registered or not), and there is no obvious way to set the profile to "private". Profiles were not found using either an external search engine (e.g. Google) or the internal Skyrock search engine. The only way to find a profile is by knowing the username.

On the blog, users upload photos and texts in the form of short articles. Blogs can be set to "secret". In that case, only friends labelled as "VIP" by the user himself can access the blog. Neither the blog nor the profile, are set to "private" by default.

Any user, including minors, can be contacted by other users, including adults. Indeed, during the tests, one of the minors was contacted by a young adult. By default, all users (registered or not, friends or not) can either send a message; post a comment on the minor`s profile or on their blog. However, privacy settings can easily be modified so that anyone, only registered users, only friends, or only best friends can post a comment on the blog. It is also possible to set one`s profile so that any registered users or only friends can post comments on the profile. However, some differences appeared in the possibilities to contact minors, though privacy settings were set to the same level. On one profile (aged 17), anyone could "send a message" and/or post a comment on the profile or the blog, whereas on the other two profiles (aged 12 and 16), it was possible only for friends.

Users can also choose to pre-validate or not comments on their blog. Even when comments are not pre-validated, Skyrock provides users with a useful mechanism that allows them to validate, invalidate or delete new comments posted on their profile of blog. However, during the test, the invalidate option was displayed but could not be chosen, even when the user chose to pre-validate comments.

[14] According to the provider an account that is flagged as "suspicious" will be removed by the moderation team if it appears that the user is really underage.

On the profile, users can choose to pre-moderate comments. Users can use the same mechanism as in the blog to validate or delete comments (the "invalidate" option is displayed as well, but is not clickable).

On the chat room, an adult user cannot invite a minor to a private conversation. In addition, users are warned in a very visible and explicit way that they shall never communicate personal information (e.g. telephone number, home address, etc.).

On Skyrock, it is possible to forward user's pictures to another SNS (e.g. Facebook). Forwarding a picture on Facebook means that the picture will appear on the Facebook wall of the user with a link to the blog article and eventually a comment. The process is simple. It is also possible for users to disable this option from the personal settings option page of the Skyrock account.

Skyrock provides a simple mechanism to block users: for instance, when a registered user sends a comment, the user can go on his/her profile and choose to block him/her by clicking on a visible option in the menu.

When receiving friends requests, users can choose to accept it (become friends or best friends), refuse it, or wait. Users are also provided with a link to visit the blog of the requester.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

According to the self-declaration, there is a "Flag this content" button to report illegal content or behaviour on the site.

The provider states in its self-declaration that a report abuse procedure can be accessed from every Skyrock webpage and whenever user-generated content appears. According to the self-declaration, the reporting procedure was tested on all age groups to make sure it was easily accessible, understandable and age-appropriate. According to the provider user reports are handled promptly within 48 hours.

The self-declaration does not refer to if user reports are acknowledged or to how users are provided with the information they need to make an effective report.

Main findings in relation to the website

Confirming the findings from the self-declaration, Skyrock provides users with an easy to use, age-appropriate and user-friendly mechanism to report inappropriate content or conduct on their site. On every blog, the user finds a button labelled "report content" ("signaler un abus"). This report form is also accessible at any time from the footer of every page. When clicking on the form, the user is asked to choose what he wants to report ("a blog, profile or group", "a problem with the user account"). Then, the user is asked what kind of problem he/she wishes to report ("fake identity", "photo stealing", "porn", "hatred, racism or insults", etc.). The mechanism is quite simple and easy to use for children and the terms employed are simple. Only at one point during the reporting procedure "legal" terms are used ("Warning! Signalling a blog that does not violate the User General Conditions is not recommended. Reminder: if your request is shown to be unjustified, we have a legal right to forward it to the authorities").

Reports are acknowledged immediately by email. During the test an offending picture of a minor (girl) and a sarcastic sentence were posted by another minor (boy) on his own blog. The girl concerned by the picture and the offensive message reported the boy`s blog (using the "report this blog" button). It took only 2 minutes for Skyrock team to send an email saying that the content had been removed from the site and to actually remove the offending content from the blog.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Skyrock states that they have mechanisms in place to prioritise and process notifications from users. Categories such as inappropriate sexual behaviour, pornography, suicidal tendencies and run away are the highest in priority. The provider also claims that illegal content and behaviour are removed immediately from the site and saved for eventual police investigation.

Skyrock refers in their self-declaration to the fact that they cooperate with French relevant law enforcement bodies and that *"extremely inappropriate contents or behaviour such as paedo-criminality, racial hate, inciting or advocating crimes against humanity are reported to the French interior Minister centralized platform (PHAROS)."*Even though Skyrock claims to cooperate with relevant law enforcement bodies, the self-declaration does not mention if they include relevant links on its website to other local agencies or organizations in order to support the process of reporting illegal content or conduct.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

According to the provider, Skyrock provides relevant, easy-to-understand, contextual warnings to users regarding their online privacy. It also provides safety tips for minors including how to manage their online images. The self-declaration further states that a range of privacy setting options are accessible and prominent at all times.

The service provider further states that *"Skyrock asks very basic private information when registering and lets users decide which kind of information they want to display on their profile or blog"*. *Skyrock also points out that it allows users "to choose with whom they want to interact: everyone, members only, friends only, best friends only or nobody".*

Main findings in relation to the website

The main privacy setting option available to users is that they can turn some or all of their articles of their blog to secret. This option is always available via the user account. By doing this, all the secret content becomes only accessible to pre-approved "VIP" friends. It is easy for children to understand how this feature works. On the privacy settings page of the blog, there is easy to understand contextual information explaining how to use the "secret blog" option. Other privacy options include the possibility to restrict interactions among users, for instance by setting one's account up so that the minor can only interact with specific users or with nobody (e.g. registered users, friends, only members of one's VIP list, nobody, etc.)

In Skyrock's profiles, optional personal information (e.g. home address, favourite music, etc.) is not required in order to sign up, but may be added to one`s profile if the user wishes to do so. If a user decides to add extra personal information, this information is automatically mapped onto the user's profile. However, users are not explicitly informed of this automatic mapping of information and, therefore, they are not made aware that this information will be made visible to users beyond their approved list of contacts. For instance, if a user chooses to add information on his/her favourite music, there is no way to set this information to private: information is missing or it is public. Consequently, the user cannot choose what specific pieces of information to make private or public.

In order to deactivate their blog and profile, users have to go the "My account" ("mon compte") page, accessible from the top of every page on Skyrock. The delete option is at the bottom of that page, in the right menu, not in the main part of the page. Users can delete their blog, their profile or their account itself. When they choose these options, they are warned that all information will be

lost (including comments, pictures…). The process is simple: users only have to enter their password and a security code.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

Skyrock maintains that they employ automated mechanisms and human moderators to review the content uploaded to the platform: Apart from a high precision image analyzer algorithm employed to review all the images uploaded to Skyrock, there are also moderators who manually review all the pictures and videos uploaded to the platform. As stated by Skyrock, all the moderators employed by the provider are older than 18 year olds; they are experienced and trained, and their backgrounds are checked when they are hired.

Skyrock claims to have mechanisms in place to prioritise and process notifications from users. Categories such as inappropriate sexual behaviour, pornography, suicidal tendencies and run away are the highest in priority.According to the self-declaration; users can also flag illegal content.

Summary of Results and Conclusions

On the website, Principles 1 and 4 were evaluated as *"very satisfactory" and* Principles 2, 3 and 6 as *"rather satisfactory".* Some areas of attention include:

- Even though the minimum age requirement to create an account on Skyrock is 12, a (fake) 9-year-old child created for this test could create a profile on the site. This finding suggests some deficiencies in the flagging system and the active manual searching of underage users referred to in the self-declaration as these mechanisms proved not to be effective enough in identifying and deleting an underage user from Skyrock[15], at least during the period that the testing lasted.
- By default, any user, including minors, can be contacted by other users, including adults. Indeed, during the tests, one of the minors created for the testing was contacted by a young adult. Users, though, have the option to restrict interaction with other users if they wish so. Privacy settings are limited (thus simple to understand) and they do not offer users the possibility of deciding which specific pieces of information to share with which users.
- If a user decides to add extra personal information (not required during registration) to their Skyrock profile, this information is automatically mapped onto the user's profile. However, users are not explicitly informed of this automatic mapping of information and, therefore, they are not made aware that this information will be made visible to users beyond their approved list of contacts.

[15] According to the provider an account that is flagged as "suspicious" will be removed by the moderation team if it appears that the user is really underage.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1		x	
2	x		
3	x		
4		x	
5	x		
6	x		
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2		x	
3		x	
4	x		
6		x	

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
STARDOLL

Brian O'Neill, Dublin Institute of Technology, Ireland
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Stardoll is the world's leading group virtual entertainment environment devoted to young women and girls. Described as a social gaming destination with a focus on fame, fashion and friends, Stardoll is based in Sweden with offices in the US, UK and Germany. Intended primarily though not exclusively for girls aged 7 – 17, the site itself evolved from an earlier website called Paperdoll Heaven. It was relaunched in 2006 and now has over 100 million registered users.[16] The site emphasizes letting girls express themselves through designing and purchasing clothes for their paper doll-like avatars. At Stardoll, users create their own MeDoll, a paper doll-like avatar, or choose from a selection of celebrity dolls and dress them up from the wide selection of fashions available. According to the provider 'Stardoll is one of few places on the Internet developed with an emphasis on girls' self-expression through fantasy and fashion play'.

Stardoll generates revenue through sale of virtual currency and the sale of advertising. It also monetizes through brand promotions that often feature branded virtual goods and in-world locations. Stardoll is growing at a rate of roughly one million new members every week. The site is now available in 21 languages; with its largest market the United States accounting for around a quarter of its overall user base.[17]

Summary of main findings

This report summarises the main findings of the tests carried out on Stardoll in the period between June 21 and June 24, 2011. Testing was carried on the various social networking features of the site using a number of accounts set up for the purpose. Membership of the site is free. However, a subscription for Community membership is required for features such as using message services, create a friends list, and access other members' guestbooks. Paid memberships were set up for four accounts, three for minors and one adult account. Safety appears to be well supported across this virtual entertainment environment. Safety information is prominently displayed and the Stardoll's One-Stop Rules provide a handy, easy to understand reminder of the code of conduct for the website. Mechanisms for reporting violations are readily accessible across the website with an easily identifiable red exclamation mark acting as a report abuse button. Blocking mechanisms are also prominent in the forum, messaging and comment areas of the site. Parents are provided with some important tools for safety protection for younger children. Parental consent is required for anyone registering under the age of 13 and by default a Kid Safe account is set up which blocks any online interaction. Parents can also cancel a Kid Safe, under 13s account at any time. For other members, private communication is limited to friends only. Profiles do not contain any identifying information. Only usernames appear on profiles and members are reminded throughout the site about not including any personal information in their profile or in online communication. Some content contained within profiles is public by default. A user's guestbook, personalised album and blog entries are public. The country of origin, age and gender of the member are also public by default. Each of these may be hidden while guestbook and blog entries may also be restricted to private or friends only. Forums and party channels (chatrooms) are by their nature public and require greater vigilance on the part of children and their parents. Tests were undertaken in situations where young people might be vulnerable, for instance, in a chatroom or in approaches made by strangers through a friend request. While it is possible for a minor to be contacted in this way, the moderation of the forum/chatroom was effective and blocking of communications proved successful. In addition, as already

[16] Ashby, A. 'Stardoll turns 5, serves over 100m users'. *EngageDigital,* April 6. Retrieved from: http://www.engagedigital.com/blog/2011/04/06/stardoll-turns-5-serves-over-100m-users/
[17] 'Stardoll Reaches 100 Million Members Worldwide'. Retrieved from: http://www.prnewswire.com. April 7, 2011

mentioned, communications are blocked for under 13 year olds with a Kid Safe account and therefore they will not be able to interact with anyone.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

Stardoll claims to educate and communicate with minors and their parents on how to navigate their website safely in an age-appropriate manner that is easy to access and understand. In order to do this, they claim to provide specific targeted materials such as a parent information guide (including "family rules"), privacy policy or kids privacy policy. However, no specific materials for educators are mentioned in the self-declaration, although external links to safety awareness institutions such as safekids.com are provided.

The signatory claims to provide clear information about what constitutes inappropriate behaviour on their service via the Stardoll code of conduct called "One Stop Rules". These include: swearing, using sexually graphic language, being racist, bullying other members, asking for personal information (including photos), etc. This information must be accepted and users must commit themselves to comply with these rules when they become members of Stardoll.

Regarding the consequences of violating the Terms, the provider claims that depending on the severity of the violation users can either receive a warning and be closely monitored or their account can be deleted immediately. In more serious cases involving criminal offences Stardoll will contact the Swedish IT crime unit who will help coordinate with relevant law enforcement agencies worldwide.

Main findings in relation to the website

Safety awareness and online safety education is a prominent feature on Stardoll's website. Parents and young people will find readily available safety and education resources in the Help section of the website accessible from the bottom of each page. A special section, called Parent Information, provides information about Stardoll and what it offers for parents who may be new to the service. It describes the safety measures available, including the restricted-feature Kid Safe membership facility. This is the default type of membership for users under the age of 13 and blocks online interaction. They may be upgraded to regular membership with parental consent. An Online Security Guide for Parents is also available which sets out guidance on safe internet use, rules and guidance about disclosure of personal information, and information about parental controls or filters. The site itself does not have a section for educators but includes referrals to a limited number of external resources specifically dedicated to family online safety and education. The information available for children is also located in the Help section and contains a series of short articles on safety and security issues. Written in easy to follow language and presented in brief question and answer articles, the safety information is accessible and user friendly for children. Some of the topics included of particular interest to young people focus on what to do if an account has been hacked, how to report bad behaviour, rules about images and etiquette online. A search facility is available in the Help section and topics are organised in visually accessible categories suitable for younger children.

The Membership Terms to which all users are required to agree on first registration are available at the bottom of each webpage. It is a long statement and presented in a way that would be off-putting for most young people. It does contain a heading 'Special Information for Parents', the primary audience, and presents information about moderation and safety on the site, account set up procedures, and essential information on personal data and privacy. Stardoll's One Stop Rules, accessed from the Membership Terms, and prominent across the website, is a short, child-friendly code of conduct which sets out expected standards of behaviour and what is prohibited on the site. The frequent reference to the One Stop Rules in help articles and in such actions as blocking users for code violation is a helpful way of reinforcing good conduct and safe online practices.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

In its self-declaration Stardoll states that no minimum registration age applies, but users younger than 13 need parental consent via e-mail to join the site and are suggested to sign up for a Kid Safe account that does not allow them to communicate with other members of the community. By means of this mechanism, the parent/carer can at any time cancel their child`s membership at Stardoll.

Regarding the mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, the provider claims not to host any "adult" content and not to have any specific sections for adults only. In addition, Stardoll states that they have several mechanisms in place to ensure that minors are not confronted with inappropriate content. These include, among others: the personal information provided by users at registration is not visible for other members; users are not allowed to upload pictures of themselves or of other people and all images are pre-moderated before appearing on the site; users can also block other members from sending messages or visiting their page. The provider further claims to moderate the site and the interaction among its members; text filters are applied to detect inappropriate language, racist or sexual content and ads at Stardoll must be age-appropriate and adequate for children. According to the self-declaration, Stardoll applies a special policy for advertising targeted at children on their website. The policy refers to the types of advertising that are allowed/forbidden on the website (e.g. alcohol and tobacco ads are forbidden) and to the importance of taking into consideration children`s vulnerability when advertising any product on the website.

Main findings in relation to the website

There is no minimum age requirement for registration on Stardoll. A child seeking to register needs to enter name and date of birth. When registering on the site, those under 13 automatically get a special category of membership, called Kid Safe that blocks communication with other users of the site. Parental consent is required to approve a Community membership of the site for all children under the age of 13. In a test registration for the service, an email was sent to the address entered for the parent, notifying them of the account set up. Parents are also informed that they may cancel membership of a child's account at any time. According to Stardoll, 'adult' content is not hosted on the site and as such there are no separate categories or sections for adult content. In testing, this was confirmed and content viewable was appropriate for all age groups. Users, for instance, are not allowed to upload pictures of themselves or of other people and all images are pre-moderated before appearing on the site. Online communication is also moderated both through the use of text filtering and by Stardoll staff. In an experiment set up for the test, accounts were set up for an adult (male, 25 years) and a minor (female, 15). The adult account was set up specifically to seek contact information from a minor. It was possible for the adult account holder to make contact with the minor in a Stardoll-hosted chatroom, but divulging personal information such as name of school attended and telephone number was blocked. Text filtering was also successfully applied when racist comments or inappropriate language was posted in comments on some of the sample accounts set up. Stardoll also operate a strict advertising policy in relation to any paid advertisements that appear on the website. According to its self declaration, direct, action driven commercial messages targeted at children are not allowed. None were observed over the course of the test.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

Regarding the tools and technologies employed to assist children and young people in managing their experience on the service, particularly with regards to inappropriate or unwanted content or conduct, the self-declaration states that only limited identifying personal information (first name, date of birth and e-mail address) is required of users at registration. This information is not visible to other members. Moreover, as mentioned under Principle 2, Stardoll emphasizes that users are not allowed to use their first name in their profile, but they must create a nickname. Age, country and gender would, by default, be visible to other users, but can be made invisible. Stardoll claims that users are not allowed to upload real pictures on the site and that

private messages can only be sent to accepted friends. Members can block other users from sending them messages or from visiting their page and they have the option to delete entries in their guest book.

Main findings in relation to the website

A range of tools and technologies are provided by Stardoll to ensure safety of children and young people on the site. Kid Safe membership does not allow under 13 year old users to access any of the communication functions of the site. Online interaction for all members is moderated and tools are available to block unwanted messages and to report users and/or violations of the code of conduct, Stardoll's One Stop Rules. Users are advised not to include any personal information on their profiles. On registration, users enter a user name, a date of birth and select an avatar (which also defines gender). From this, age, gender and country of origin are automatically entered on their profile. Users may then complete a free text 'About Me' presentation located on their individual profile page. Profiles of minors are not searchable on the service or through external search engines. By default, all profiles, including the profiles of minors, are visible to all users, even those beyond the approved friends' list. A public version of the profile which contains the username and avatar but no personal information, is visible to non-registered users but only if they have the URL. A link to this public profile is placed on the user's home page allowing them, for instance, to share it with non-users of the site. Within the Stardoll virtual environment, profiles, which may include any (identifying and/or non-identifying) information entered by the user in the 'About Me' presentation, are visible to all registered users. Each profile also contains a guestbook in which visitors can enter comments. Users can also maintain a blog as part of their profile to which others may add comments. An option is available in privacy settings to restrict the guestbook and blog to friends only, to pre-moderate comments or to keep it completely private. It is also possible to hide a user's gender or age on their profile. By default these are displayed. Only friends may send private messages and use the chat function. All users may send friend requests and also have the ability to block other users.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

The self-declaration states that users can report content to the Stardoll moderators and/or they can delete content themselves (e.g. an entry in a user's own guest book). Members can also block other users from future contact. Stardoll provides abuse reporting tools wherever there is textual user-generated content (e.g. chat, guestbook messages, text presentations, etc.). The self-declaration states that the reports are dealt with within 48 hours. The consequences of the reporting vary depending on the severity of the violation. For instance, a reported user may simply receive a warning or in more serious cases, they may be expelled from the site and their member account could be deleted. No information on if users are provided with an indication if their reports are acknowledged nor information on how reports are typically handled was found in the self-declaration.

Main findings in relation to the website

Mechanisms to report violations of Stardoll's code of conduct, its One Stop Rules, are available in all locations where there is user-generated content and where a user may be subject to harassment or abuse from other members of the service. A report flag – the red exclamation mark placed within communications function in the message service – is available in the chat message box and in the comments areas. Clicking the report flag provides the user with an option to block the sender and/or to continue with a report about the violation. Information about reporting code violations is available in the Help section. Users are reminded when filing a complaint that false reports or abusing the report function may result in termination of an account. Testing this function involved submitting a report about offensive comments posted to a blog entry on the account of a minor (not a real account). The process of submitting a complaint was easy to follow and no difficulties were experienced. In reporting, the user was offered the option block the offender in the first instance and/or continue with submitting a complaint. The information requested was specific and offered a set of straightforward options regarding the object in question (a private message, a comment) and the nature of the abuse (offensive language etc.). Confirmation was given that all complaints are treated seriously and acted

upon within one day. The sender was also informed that they would not be contacted about the complaint unless further information is received. Possible actions include removing of the offending content, and warnings or termination of the subject of the complaint. In this case, the offending content was removed. No further communication was received nor did the creator of the offending comments receive a warning.[18].Members may also use the 'Contact Us' at the bottom of the each page to submit a report of a more general nature.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The provider states in its self-declaration that if users slightly violate Stardoll One-Stop-Rules, the member in question will receive a warning and will be closely monitored by Stardoll staff by means of an "internal warning list of reported members". If the violation is severe, "the reported account will be deleted immediately". If required, further details regarding the reasons for deleting the account, may be sent to the reported user and further investigated by Stardoll customer service staff. Stardoll claims to count with trained customer service staff and moderators who elaborate appropriate responses to reports and flags. According to the provider, members of Stardoll staff and moderators "regularly meet to calibrate and discuss children`s behaviour and the necessary actions to be taken".

The self-declaration mentions that user`s reports are dealt with within 48 hours and in case of severe violations the reported account will be deleted immediately. Depending on the severity of the violation users can either receive a warning and be closely monitored or their account can be deleted immediately. In more serious cases involving criminal offences the Swedish IT crime unit is contacted to help coordinate with law enforcement agencies worldwide.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

Stardoll claims that keeping the identities of their members protected is a "high priority". Indeed, Stardoll emphasizes that they do "not accept any identifying information being exchanged between its members and such information is taken off the site. Members also run the risk of being expelled from the site in cases where they post such information". In addition, the provider claims that no personal data from its members is transferred to third parties. As stated under Principle 3 and in the self-declaration, Stardoll has taken several measures that can minimize the risk of profiles of minors being found online, for instance only limited identifying personal information (not visible for other members) is provided by users at registration and users are not allowed to use their first name in their profile.

The self-declaration states that users of this SNS are provided with a range of privacy setting options including, among others, the possibility for users to make certain information from their profile invisible to other users, the option to block other members from sending them messages or viewing content in their pages. The provider also states that users are warned not to give out any identifying information on the site. This is done via the Kids privacy policy and through the Online Security Guide.

Main findings in relation to the website

In general, profiles are accessible only to registered users within the Stardoll environment. Users are informed when they first set up an account and reminded in help articles about never giving out personal information such as real name, address, email, or telephone number. Some automatic mapping of information collected on

[18] According to Stardoll, the submission of a first report might not result in a warning. However, several reports will result in a warning being issued or in deletion of the offender's account

registration takes place and a user's profile displays by default age, gender and country of origin. The profile template does not contain fields for personal information and only a username, age and gender are visible. A text box called 'About Me', in which one can enter descriptive information, is available on the profile page and is visible by default to all registered users. Users are advised but not prevented from entering personal information. In the tests undertaken, for instance, personal information including name, age and city of location were entered into the 'About Me' description and these details were available to all registered users of the site. These findings suggest that even though Stardoll does "not accept any identifying information being exchanged between its members", it is possible for users to exchange or share identifying information with all other registered users of the site by adding information to the "About me" section. Other personalisation of the user's profile does not involve any potentially identifying information and is achieved through creative design, using the tools supplied for creating an avatar and stylising its environment. Privacy settings, accessible from the My Account tab, allow for control of visibility of information displayed. Here it is possible to hide details such as country of origin, gender and age, which are made visible by default. User content such as the profile guestbook and blog are again by default open to all to post, but may be made completely private or restricted to friends only. Only friends can see the online status of users through the chat function and only friends are able to send private messages. It is not possible to restrict a full profile to either 'friends only' or to nominated friends. Some information and functions may be restricted but all other aspects of a user's profile remain visible to all and for this reason ensuring that profiles do not contain any personal information is essential. Deleting a user's account is easily achieved. A link is provided in the help section which deletes the account. Information is provided in the Membership Terms in the section on Personal Data and Privacy Policy on data retention as prescribed by applicable law. This is intended primarily for parents and younger users would have difficulty understanding its meaning.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

In order to identify and review prohibited or illegal content or conduct, Stardoll claims to operate extensive moderation (via the trained customer service staff) on the site and also to employ automated tools, such as filtering tools for inappropriate language, racist or sexual content.

Even though the self-declaration indicates that "the customer service staff and moderators are trained in appropriate responses to reports and flags", it is not clear from the self-declaration if staff are in real-time contact with children or young people. In case they were, no information is provided in the self-declaration regarding the steps taken by Stardoll to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people.

Summary of Results and Conclusions

On the website, Principles 1, 2, 3 and 4 were assessed as very satisfactorily implemented. Principle 6 was assessed as rather satisfactory. The main strengths of this SNS are that safety information is prominently displayed and the Stardoll's One-Stop Rules provide a handy, easy to understand reminder of the code of conduct for the website. Mechanisms for reporting violations are readily accessible across the website with an easily identifiable red exclamation mark acting as a report abuse button. Blocking mechanisms are also prominent in the forum, messaging and comment areas of the site. Other positive aspects include the fact that online communication is moderated both through the use of text filtering and by Stardoll staff. In addition, profiles of minors are not searchable on the service or through external search engines. Finally, privacy settings, accessible from the My Account tab, allows for control of visibility of information displayed while deletion of an account is easy to accomplish.
Some areas of attention include:

- Even though the self-declaration states that Stardoll "does not accept any identifying information being exchanged between its members", it is possible for users to share identifying information with all other registered users of the site by adding information to the "About me" section. In

other words, any (identifying and/or non-identifying) information entered by the user in the 'About Me' presentation is visible to all registered users.

- Users can't restrict a profile to friends only.
- It is possible for a minor to be contacted via the forum/chatroom, but the moderation of the platform was effective and blocking of communications proved successful.
- All users may send friend requests, but only friends may send private messages and use the chat function.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3		x	
4		x	
5	x		
6		x	
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
6		x	

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
MICROSOFT WINDOWS LIVE

Brian O'Neill, Dublin Institute of Technology, Ireland
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Windows Live is the collective brand for Microsoft's suite of free web services and software applications designed to allow users to store and organise their communication activities and digital content in one place. The majority of the services are web applications accessible through a browser. Windows Live Essentials is a set of software programmes which are downloaded and installed on users' PCs and include a Family Safety application. First announced in November 2005, Windows Live brings together a wide range of products and services including email, instant messaging, online storage and photo sharing, as well Office Live online collaboration. Closely linked to the Windows operating system but available separately and on a cross-platform basis, Windows Live is primarily a suite of productivity and communication tools with social networking functionality. According to Microsoft's Self Declaration statement, Windows Live services are general use services and are not primarily directed at children under the age of 18.[19] However, services such as Windows Live Messenger, the instant messaging service, has over 300 million active users across the world and is popular with children while Windows Live Hotmail is, according to comScore, the world's largest web-based email service with nearly 364 million users.[20]

Summary of main findings

This report summarises the main findings of the tests carried on Microsoft Windows Live in the period June 11, 2011 to June 16, 2011. Windows Live is a web-based set of applications and social networking environment that includes email, photo and file sharing. While not described as designed for children, it incorporates Windows Live Messenger, an instant messaging service that remains very popular among young people.[21] It also includes the separate Windows Live Family Safety application. This is a free, desktop-based software filtering tool that needs to be downloaded from the website and installed on each computer used by the child to be effective. Safety information and enabling tools and technologies are prominently featured in the different applications and services offered by Windows Live. The Windows Live Terms of Use and Code of Conduct statements provide users with easy to understand information about the services, including safety information. There is a help site, accessed from the main menu to a dedicated Windows Live Family Safety Help Center though this only refers to the separate parental controls software and not to safety in general. Additional resources and educational materials are provided on Microsoft's central safety and security website. This is not as easily found. There is a link to it from the Windows Live Microsoft Service Agreement (under Parental Controls) and it does contain child and teen-oriented materials. Not all users will be aware of its existence, however.

Testing was undertaken on the various services offered on Windows Live both with and without the use of the Windows Live Family Safety software. The available tools for reporting abuse or violations are accessible, easy to use, and were found in tests to be effective. Privacy settings across the range of services, which includes instant messaging, email, profile, photo and file sharing, were likewise found to be easy to set up and to maintain. Some difficulties were encountered in restricting information within a profile's contacts list (see Principle 3 below) but in general, the website's default safety settings are effective in ensuring minors' personal information is secure and blocked from external access. The Family Safety software provides added protection

[19] MICROSOFT Windows Live, EU SNS Safer Social Networking Principles Self-declaration Form 5th November 2010.
[20] http://www.microsoft.com/presspass/newsroom/msn/factsheet/hotmail.mspx

for parents in supervising online communication and web access for child and teenage users. The software is easy to install and integrates well with the Windows operating system. It does require more input from parents in operating and maintaining a parental controls application and must be installed on the computer used by the child to be effective.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

The provider states in its self-declaration that the "primary online safety education site is centralised and broadly available to *all consumers"* via the "protect site". The provider also claims to provide "Kid-specific social networking guidance" (targeted at parents) and other safety guides and materials (for educators and other consumers) through the corporate website (e.g. a safety and security tips blog, general social networking tips, monthly safety and security newsletter for parents and consumers in general, an online safety channel on YouTube, etc.). However, it is not clear from the self-declaration if any of this information is specifically targeted at children or how this safety information (available on the corporate website) is made available to children and young users via Windows Live. Microsoft further claims to offer plenty of educational materials and participate in a number of initiatives that support the education of parents, carers and teachers, as well as that of younger users regarding online safety. According to the self-declaration, free Family Safety features are available via Windows Live.

The signatory states in their self-declaration that they provide a Code of Conduct with clear information about "various prohibited uses of the Windows Live services" and the consequences thereof. These prohibited uses include, for example, uploading, transmitting, distributing or facilitating any content that depicts nudity, that incites, advocates or expresses pornography; soliciting or collecting personally identifiable information of any minor, etc. The provider claims that the code of conduct, the Terms of use and the Privacy link are available from every page and there is a link to the Terms of Use and privacy Policy on the sign-in page as well. According to the provider, "all users must review and accept the Microsoft Service Agreement (also known as "Terms of Use")" when they register to the service. The Terms of Use incorporate the Windows Live "Code of Conduct" and the privacy Statement.

Main findings in relation to the website

The Windows Live environment is an application-rich web space in which users organise their digital content and online interactions through the use of email, instant messaging, photo and file sharing, and accessing other programmed content on MSN. Although the safety information and features are easily accessed across these diverse services, within the Windows Live environment safety information is not specifically targeted at children. The primary focus in Windows Live is given to parents and other adults responsible for children's internet use. Users are referred through the help menu to the Windows Live Family Safety application which must be installed on the PC to take effect. Information and video tutorials aimed at parents guide users through the use of parental controls. Additional resources, not directly accessible from Windows Live (except via a link in the Microsoft Service Agreement), are mentioned in the provider's Self Declaration statement and include central Microsoft Security and Safety web pages, a newsletter, blogs, YouTube and other downloadable educational resources. Topics addressed include social networking, privacy settings, and personal information security presented in clear, user-friendly language. Further information can also be found in the Windows Live Solution Centre, accessed from the Help link in the website footer. This includes a series of FAQs and a facility for registered users to ask questions.

The Windows Live Terms of Use are easily accessed from each page of the website. The Microsoft Service Agreement, while clearly laid out and visually accessible, is a long and complex document requiring a significant amount of scrolling down the webpage. The Code of Conduct is much more succinct and outlines in a very straightforward fashion allowed and prohibited uses of the services, rights and responsibilities of users, simple instructions about how to report violations of the code, and implications for abuses of the service. The Terms

of Use provide a link to Microsoft's central safety and security website (http://www.microsoft.com/security/default.aspx) which, while extremely informative and helpful, will be difficult for users to find unless they are already aware of it. No other link to this resource could be found within Windows Live.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

Even though Windows Live claims not to have any specific sections/services for adults only, the provider claims to limit the availability of some functionalities to younger users and to provide parents and guardians with free "Family Settings" that help them manage their children`s online and offline activities. For instance, parents can decide if their child`s information can be shared with third parties or not. In the self-declaration, the provider also refers to a number of usage prohibitions applicable to their services. These include depicting nudity, inciting, advocating pornography, vulgarity, obscenity, soliciting or collecting personally identifiable information from minors, etc. Windows Live claims to review all hosted images by use of filters to detect pornography. According to the provider, minimum age requirements and/or parental consent may apply depending on the laws of each country where the service operates. If minimum age requirements apply, Windows Live claims to place a session cookie on the registration page so that "prospective users cannot change their age if their initial age is below the age required in a specific country for age verification."

Regarding the functionalities put at the disposal of content providers, partners or users in order to label, rate or age restrict content where appropriate the provider states that they provide parents with "simple controls to monitor and protect their children". These controls would allow them to set safer searching across all major search engines, "safer browsing with enhanced filtering choices" and safer social networking. The provider further claims that if parents add their child's Windows Live ID to Family Safety, no paid advertisements will be displayed on live.com websites (at least when the child is logged into Windows Live). The signatory also claims that Microsoft Privacy Policy "provides parents with access to their child`s personal information (…) and gives parents the ability to delete the information ad opt out of future collection of the child`s information."

Main findings in relation to the website (without Family Safety enabled)

According to Microsoft's Self Declaration statement, Windows Live are general use services and are not primarily directed at children under the age of 18. As such, specific age restrictions are not applied to content hosted on the service. The Windows Live Code of Conduct states that services are designed for individuals of 13 and over. However, where local laws allow, it is possible for under 13s to use the services. On a PC without Family Safety settings applied, it was possible to register an account for a minor under the age of 13. This did not require parental input and no restrictions were placed on the account set up. Microsoft ensures that services are age-appropriate by automatic blocking of any content that contravenes the Windows Live terms of service.

Main findings in relation to the website (with Family Safety enabled)

Windows Live strongly advocates the use of parental controls as a means of ensuring that services are age-appropriate. The Windows Live Family Safety is a software application available for download from the Windows Live website. The software needs to be installed by a parent on each computer used by a child in order for parental controls to take effect. With the use of Windows Live Family Safety parental controls, it is possible, for instance, to limit a minor's internet access to just child-safe websites; to require approval for online friends; to specify who is able to contact the child such as by email or instant messaging; and to block access to other designated websites (e.g. Facebook and Myspace). For the purposes of testing, Windows Live Family Safety was set up for a child account. A range of settings were tested including "Child Friendly", which blocks adult sites and online communication; "General Interest" which allows a wider range of web access but

blocks social networking; and "Online Communication" which allows social networking but also blocks adult sites. One of the tests conducted consisted in limiting access to child-friendly websites suitable for a nine year old and blocking access to other sites that might not be deemed age-appropriate. All of these controls were found easy to install and operate; they proved to be effective in providing a high degree of parental control over all aspects of online search, web access and online communication.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

In its self-declaration statement, the provider claims to employ a number of tools to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct. For instance, according to the provider, the profiles of users registered as under 18 are not searchable and their Windows Live default setting is set to "friends" which means that only contacts that the user has added can view their information. According to the provider, users can control who can access their full profile by, for example, being able to block other users or by rejecting friends' requests. The signatory claims that users can also change or conceal their online status and that they can allow access to their profile to specific users or groups, for instance, groups of friends, networks, etc. The self-declaration also refers to other functionalities put at the disposal of users including the possibility to "specify who can post and view comments on their shared photos, files, blog posts or guestbook" or the option to determine who can tag people in their photos and which other people can tag them in photos.

The service provider claims to educate parents about the uses and benefits of parental controls through the free available Family Safety and the tutorials that accompany them. The provider states that Family Safety focuses on safer social networking, safe searching across major search engines, and safe browsing with enhanced filtering choices.

Main findings in relation to the website (without Family Safety enabled)

Windows Live was first tested accessing its web-based services without the use of Family Safety parental controls. The Windows Live website provides a range of tools and technologies that are intended to ensure a safe social networking environment and to empower users to protect their privacy and personal information. Privacy settings for accounts of minors are by default set to 'Limited' and profiles of under 18s are not searchable by entering common search terms (e.g. age, name, etc.) via internal nor external search engines, although it was possible to find young users via their profile URL, for instance, by clicking on the profile of a minor contained in a friend's contact list.

One of the tests undertaken was to assess if it was possible for a minor to be contacted by people (registered users and non-registered users of this SNS) beyond their approved "friends" on their contact lists. Testing was carried out without the use of the Windows Live Family Safety parental controls – in other words just using the default settings for an under 18 account. Even though, the provider's self-declaration states that the default permission setting for Windows Live accounts for users under 18 is set so that only "friends" can view their information, testing demonstrated that information contained on a minor's profile, for example, a user's full name, information about schools attended, work and education, and interests/hobbies depending on how much detail a user has chosen to post - is visible, using the default setting, to other users beyond the minor's approved contact list[22]. In this test, the adult stranger, in this case a friend of a friend[23], was also able to send a friend request to a minor though it was not possible to make contact through other means, for example, via private message or commenting on pictures, etc.

Users are advised when accepting friend requests to limit the access to information a friend can see about them. A category of "some friends" is a subset of the contacts list and does not include friends with limited access. Friends with limited access can see public information provided on the profile; "some friends" can see

[22] For the sake of this assessment, "the minor's approved contacts list" is equivalent to "only friends".
[23] "Friends of friends" do not belong to the user's approved list of contacts and, therefore, even though they are befriended with the user's friends, they still constitute a group of potential strangers.

full profiles, including contact information. As declared in the provider's statement, it is possible for users to delete posts, remove tags or delete photos/videos on their profile. They can also by adjusting their privacy settings restrict access and control information on their personal profile such as deciding who will be able to view activities, photos and files, and contact information. Blocking of unwanted friend requests and reporting as spam is also easily achieved. Profiles of users under the age of 18 are also not searchable in any of the main external search engines.

Main findings in relation to the website (with Family Safety enabled)

Testing was also undertaken with the use of the Windows Live Family Safety application. The default settings for "Online Communication" were applied which allow access to general interest websites, allows social networking but blocks adult content. The controls are user-friendly, effective and easily accessed in the parental controls section of the PC. By default, with the use of Family Safety controls, profiles of minors are only visible to their approved contact list. Communication is blocked for any users not on their friends list. Emails from people who aren't on the list won't be received nor can Instant Messaging be used with anyone outside the friends list. The same test as above was conducted whereby an adult stranger attempted to make contact with a minor. In this case, the profile of the minor's account was not accessible nor was it possible to send a friend request. The default settings mean that parents control the minor's contact list and must approve any new contact added. Safer default settings were therefore available with the use of Family Safety controls than on the Windows Live website on its own. A similar level of safety may be achieved on the website but it requires additional input on the part of the user and finer adjustment of profile privacy settings for the same effect.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

Regarding the mechanisms employed to report inappropriate content, contact or behaviour that violates the Terms of Service Windows Live claims to provide a report link at the bottom of web pages on services where users can view, post or share user-generated content. Users can also report abuse via the menu in Windows Live Messenger or from the Windows Live Messenger application. "The Windows live web services include a "Report Abuse" button on pages where users can post, share or view other users` content."

The provider states that the report abuse mechanism ensures that "the service handles *priority* abuse issues related to content users post or share via the Windows Live services". This mechanism allows the appropriate flagging, reviewing and handling of issues such as child pornography or exploitation, as well as other priority safety fields (not specified in the self-declaration). The self-declaration further states that users are encouraged "to provide as much detail as possible regarding the abuse or offensive behaviour". No information was found in the self-declaration regarding if the procedure to report inappropriate conduct or content is easily understandable for children or if it is age-appropriate.

Main findings in relation to the website

Reporting abuse is available by an easily accessed link on each page of Windows Live and is the principal mechanism for reporting abuse, offensive behaviour or violation of the code of conduct. A simple to complete form is provided asking users to supply relevant details of the incident or violations concerned. While Microsoft does not undertake to reply to every report, confirmation is given that appropriate action will be quickly taken. For this test, a sample complaint was filed asking for help to remove offensive images on a minor's profile. A question was also posted on the Windows Live Solution Centre again requesting information about how to remove images. A reply was also received within one day. The images themselves were removed within two days and a response by email to the complaint was received five days later.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

The provider ensures that they have mechanisms in place to respond to notifications of illegal content or conduct. These include the "Report Abuse" link and "Feedback" accessible from the service. The provider also states that reports of abuse (potentially involving illegal content or conduct) are responded and that they work "in close cooperation with law enforcement and government agencies in response to lawful request". The self-declaration refers to a number of law enforcement agencies with whom the provider liaises, e.g. the INTERPOL. It also refers to the initiatives they`ve supported, for instance, the creation and the provision (at no charge) of the COFEE software (Computer Online Forensic Evidence Extractor) to law enforcement around the globe.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

Windows Live claims that users of this SNS are provided with a range of privacy setting options so that they can choose a default privacy setting from three privacy settings for their Windows Live profile, namely public, limited or private. By means of the so-called "privacy selector" the provider claims to allow users to determine their permission choices to share personal information and activities. The options include: everyone (public), "my friends and their friends", "friends", "some friends" and "just me".

The signatory further states that users can also use "Advanced Privacy" settings which offer intuitive and user-friendly granular settings that allow to set permissions ranging from most to least restrictive. According to the provider, no automatic mapping of information takes place on their services other than the username selected for the creation of a Windows Live ID. The provider also claims that users are provided with the privacy settings page which allows users to view or to change the privacy settings used and which can be visited at any time by clicking a link on the user`s profile page.

Main findings in relation to the website (without Family Safety enabled)

The Windows Live privacy statement is accessible at any time from the footer of the website. The only information that is automatically mapped onto the user's profile from account registration consists of name and surname. Users may optionally enter further details such as contact information (email, telephone, IM), schools attended, hobbies and interests. Instructions on how to delete an account are found relatively easily in the account management settings located within the profile page. Clear information is also provided about policies on deactivation and deletion of accounts. Users are informed that they may deactivate their account at any time by request. Deactivation rather than deletion is effected in the first instance as an email address is associated with the account. Once there is no log in after 270 days, the account is permanently deleted and all stored messages and content are removed.

The privacy settings for the account were tested both with and without the use of Family Safety parental controls. Privacy settings, providing options to select and modify permissions to access content on a user's account, are accessed in both cases by clicking on the user's profile page. These are user-friendly, easy to access and to adjust as required to each user's preference. When used without Family Safety parental controls, three main types of settings 'Private', 'Limited' and 'Public' are available. By default, privacy settings for minors are set to 'Limited' i.e. the user's profile containing any descriptive information about general interests, occupation and location is visible to all. Other information such as status, contact information and access to photo albums is restricted to friends only. Users can further adjust settings using either a basic or advanced mode. The former is an easy to use checkbox selection that defines the principal privacy modes. The more advanced settings allow users to modify individual settings with a finer degree of control over which aspects of a user's information are visible and the kinds of online communication that are allowed. Windows Live advises users to enable additional settings to limit access for certain information to 'close friends'. These were easy to

manipulate, allowing users greater control over their personal information. However when contact information was set to be accessible to only 'close' friends, this was found to be visible also to the whole list of friends.

Main findings in relation to the website (with Family Safety enabled)

With Windows Live parental controls enabled, the account's privacy settings are managed in the first instance through the Family Safety application. Greater levels of privacy are enabled by default using the parental controls facility. For instance, profiles of minors are only visible to friends and may not be made public or visible to all. A user may also choose to further restrict access to certain parts of the profile (contact information, interests, photos) to some friends or to make some parts of it invisible. Contact management is also set by default to be controlled by parents who can then choose which communications services to allow and who the child can communicate with on Windows Live Messenger and Windows Live Hotmail. The default setting may be changed to allow the child to manage their own contacts but this still allows the parent to monitor the contact list. In tests, with Family Safety settings enabled, only friends could access and contact the test account of a minor. The profile was listed as private for other users and no information was visible.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

The provider claims to employ a range of automated technologies to ensure the integrity of their services and to allow users to report any violations of their Terms of Use. The provider also affirms that when they become aware of a violation to their terms of use or code of conduct (e.g. through user-generated reports), prompt steps are taken "to remove and take down illegal or prohibited content/conduct". The provider states that they have "established and trained personnel on (their) global processes and standardised practices to ensure that (they) respond in a consistent manner and to meet all applicable laws and regulations worldwide related to this subject".

Summary of Results and Conclusions

On the website, Principles 1, 2, 4 and 6 were assessed as very satisfactorily implemented and Principle 3 as rather satisfactorily implemented. The main strengths of this SNS are the availability of safety information and features that are easily accessed across diverse services. Another positive aspect are the tools provided to ensure the services are age-appropriate for the different categories of users. For instance, the Windows Live Family Safety downloadable application is an effective web filtering and parental control application that provides a high degree of flexibility for parents in monitoring and supervising children's internet use. However, its use requires extra input on the part of the parent to ensure maximum levels of safety and must be installed on the PC used by the child to be effective. Reporting abuse on the platform is easily available and efficient. Ready access to privacy settings by clicking on the user profile was found to be very user-friendly, effective and easy to manipulate, allowing users a high degree of control over their personal information.
Some areas of attention include:

- Lack of safety resources specially targeted at children rather than to the general public.
- Additional resources and educational materials provided on Microsoft's central safety and security website are relevant, but they are not as easily found via the Windows Live services tested.
- According to the provider's self-declaration, only friends should see a user's activity and information. However, information contained on a minor's profile, for example a user's full name, information about schools attended, work and education, and interests/hobbies depending on how much detail a user has chosen to post - is visible, using the default setting, to other users beyond the minor's approved contact list.
- During the tests without the use of Family Safety controls, contact information was set to be accessible to only 'close' friends. However, this was found to be visible also to friends.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	X		
2	X		
3	X		
4		X	
5	X		
6	X		
7	X		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	X		
2	X		
3		X	
4	X		
6	X		

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
MICROSOFT XBOX LIVE

Brian O'Neill, Dublin Institute of Technology, Ireland
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

Xbox LIVE is the online gaming and digital media entertainment service of Microsoft. First launched in 2002, Xbox Live has nearly 25 million members across 35 countries.[24] The use of the service requires an Xbox 360 console as well as a broadband internet connection: Xbox Live as a gaming and entertainment service now spans the Xbox360 console itself, and the PC (Xbox.com and Games for Windows Live). The Xbox 360 console is the primary platform of the service. This is where users play console games, play online and access movies, other entertainment available through Xbox Live. On the website, users can view and edit their profile, access the Xbox Live Forums, adjust their safety settings and preferences, and search for information about games. The same account and username (gamertag) applies in both cases. Xbox Live membership is available in three main forms: Xbox Live Free provides access to entertainment services and content via broadband connection; Xbox Live Gold Membership includes multiplayer online gaming; and Xbox LIVE Gold Family Pack is a family bundle for up to four 12-month Xbox LIVE Gold memberships. The Xbox LIVE service is intended for users of all ages. Functionality may be limited for younger users and parental controls are provided for managing children's use. Xbox LIVE requires parents or guardians to create accounts on behalf of children.

Summary of main findings

This report summarises the main findings of the tests carried out on the Xbox Live service accessed through the Xbox 360 console and Xbox.com website in the period from June 11, 2011 to June 19, 2011 using an Xbox Live Gold membership. Safety controls and supporting information across the Xbox Live gaming and entertainment services were found to be extensive and effective. Safety education is presented in a way that parents and young people will find accessible and user friendly. In general, resources are easy to find despite some initial difficulties experienced in locating safety content. The Xbox Live Code of Conduct which applies to both the console and the website is a clear and succinct statement of the standards of behaviour and content required of its users. Players can easily report violations of the code and Xbox Live undertakes to review every complaint filed. Privacy controls are easy to set up and modify as required both on the console and on the website. Parents are required to give consent for registration of accounts of hereafter, parents choose the level of permissions they wish their children to have. Xbox Live users control the information placed on their profile and to whom it is visible. Unwanted communications may be blocked and/or restricted, and friend requests are controlled according to easily accessed safety settings.

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

According to the provider, Xbox Live provides plenty of comprehensive online safety content which is "available and easily accessible through www.xbox.com". The most comprehensive and context relevant information is also available through the Xbox console. This includes videos with tutorials and information on how to use the Xbox Family Settings, privacy settings, and abuse reporting mechanisms. The provider further states that "primary online safety education site is centralised and is broadly available to *all consumers"* via the corporate

[24] MICROSOFT Xbox LIVE EU SNS Safer Social Networking Principles Self-declaration Form , 5th November 2010

"protect site". According to the provider, other types of safety resources are also available through this corporate website. These include a safety and security tips blog, general social networking tips, an online safety channel on YouTube as well as a monthly safety and security newsletter for parents and consumers in general. From the self-declaration it is not clear, though, if this safety information is specifically targeted at children and younger audiences or how this safety information (available on the corporate website) is made available to children and young users on the Xbox Live website and/or the Xbox console.

The signatory states that they provide clear information about what constitutes inappropriate behaviour on their services and the consequences thereof, e.g. if a player is caught cheating or "griefing" (making it hard for others to play), the offender can be muted or suspended for a certain period of time and the offender`s account and/or console may even be banned from Xbox LIVE permanently.

Microsoft claims to have education partnerships with a broad range of institutions and to offer plenty of educational materials and participate in a number of raising awareness initiatives that support the online safety education of families, carers and teachers, as well as that of younger users.

Main findings in relation to the website and console

Xbox Live, through its website and on the Xbox 360 console, provides extensive information and educational resources aimed at raising awareness of internet safety and privacy protection. As an online gaming and entertainment service with social networking features, the information provided is practical in nature and intended to provide users with the necessary skills to use Xbox services effectively and in a safe manner. Safety and educational resources are targeted separately at parents and at teenagers.

Some difficulties were encountered during the tests in locating safety resources, but once identified were found to be comprehensive and informative. A link from the main menu to the Family Center, the Xbox.com location for safety information, didn't work in the test.[25] It was also necessary to perform several searches of Xbox Live Support to locate further resources. A special online safety website with a focus on gaming is provided as part of the Xbox Live service (http://playsmartplaysafe.eu/). Once registered and logged in, a link is provided on the welcome page of the website. Microsoft's primary online safety website (http://www.microsoft.com/security/default.aspx) also contains additional information for parents and young people on all aspects of internet safety, privacy and security.

The safety information available via the console is more limited. The 'Xbox 101' video tutorials, mentioned in the provider's Self Declaration statement, could not be found on the console. A web search revealed the videos were located in the Community section of the Xbox.com website and on You Tube. The content itself was informative and very practical in nature, ideally suited to the gaming environment and the target audience. Other useful resources available from Xbox.com include fact sheets, testimonials from Xbox Family Ambassadors, community help resources and a safe gaming guide. Materials for download include a *Family Guide to Video Gaming,* a checklist for parents on digital technology, and quizzes about young people's gaming habits. There is also a dedicated safety website and series of FAQs for the Kinect controller. Two key audiences stand out as targeted by the safety information on Xbox Live: parents or those responsible for setting up younger children's Xbox accounts; and teenagers or young adults, the main users of Xbox services. There is little evidence of safety information specifically designed for younger children. The available resources are, however, written and presented in a very user-friendly way and will be both informative for new users of all ages and effective in providing solutions and guidance for more experienced users. There are useful links to external sites and organisations and a link is available to the PEGI (Pan European Game Information) website on the footer of each webpage providing additional information and resources.

Terms of Use for Xbox Live are easily accessed from any page of the website linking to two separate pages outlining the Xbox.com Service Agreement and a Code of Conduct. The latter is an exemplary, jargon-free statement that gives users clear information about what is expected of them, the consequences of violations of the code, and of potential risks they might encounter. Terms of Use are somewhat more legalistic in form but are clearly laid out and presented. Accessing the Terms of Use on the Xbox 360 console is less easy. After much

[25] http://www.xbox.com/en-GB/Live/Home?friends_and_family

searching, they were located via the Dashboard under Account Management settings. Reading text via the Dashboard has natural limitations: It is harder to read and involves scrolling on a single page. There is no specifically adapted version of the Terms of Use or the Code of Conduct for children or younger people.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

Regarding the mechanisms through which the service provider ensures limited exposure to potentially inappropriate content and contact for children, the provider claims to limit the availability of some functionalities to younger users (e.g. more conservative default profile settings apply or parental permission is required to perform certain actions). Besides, the self-declaration mentions that mature-rated content such as certain games can be blocked and/or be hidden from minors. No minimum age requirements apply, but a birth date and parental consent are required for minors to sign up to Xbox LIVE. For users under 18, these data are verified by entering credit card details. As stated in the self-declaration, "Xbox live requires parents or guardians to create accounts on behalf of their children accounts, and requires that the parent or guardian is responsible for the use of the account by the child."

As regards the functionalities put at the disposal of content providers, partners or users in order to label, rate or age restrict content where appropriate, the provider claims that Xbox allows parents or guardians to specify which categories of games and movies their children are allowed to access. This is achieved by means of "Family Settings" that help them manage their children`s online and offline activities. Besides, the console can be configured to restrict online gaming, communication and the sharing of personal information e.g. to only approved friends or to require parental approval for new friends. Furthermore, the console recognizes several game and video rating systems, e.g. PEGI.

Main findings in relation to the website and console

There is no minimum age for Xbox or Xbox Live services. However, extensive tools are provided to ensure the services are age-appropriate for the different categories of users. These may be used to limit content that can be viewed or played, protect privacy or limit the amount of time spent on the console and on Xbox Live. The two main ways of enabling family settings are the "Family Centre" settings in the case of Xbox LIVE Family Pack subscribers, and console "Family Settings" for individual accounts. Family settings are accessed via the welcome screen on the Xbox 360 console and are accessible at any time. The same settings can also be monitored and controlled online at Xbox.com. Three main default settings are presented for child, teen and adult accounts respectively. Accounts for under 18 year olds need to be set up by an adult and are verified by entering valid credit card details. Parents are also required to be responsible for child or teen accounts and to authorise any amendments to default settings. A valid Windows Live ID is required to set up Xbox Live access. PEGI and BBFC (British Board of Film Classification) ratings are used for games and movie content and permissions may be set within console family settings.

During the period of testing, the console and online safety settings proved to be easy to set up and use, and effective in restricting access to content that may not be age-appropriate. Exceptions for game play or communications purposes could be added if required such as by allowing an age-restricted game or approving a friend request with parental approval. Despite the very diverse services incorporated within Xbox Live such as gaming, entertainment, film and video content, online communication, online and console safety settings and parental control features remain readily accessible, are easy to set up and manipulate as required for the particular service.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

As regards the tools and technologies employed by the service provider to assist children and young people in managing their experience on their service in particular with regards to inappropriate or unwanted content or conduct, the provider claims to have taken a number of steps in order to ensure that private profiles of users

registered as under the age of 18 are not searchable, for instance, even though gamer tags can be searched, blocked profiles (i.e. users younger than 13) only reveal minimal information (gamer tag and gamer score) and 13-18 year olds can only share their profile with friends. According to the provider, profile sharing for under 13 year olds is blocked and 13-18 year olds can only share their profile with friends. Besides, the self-declaration states that adding new friends is blocked, by default, for all under 18 year old children and parental approval of a child`s list of online friends is needed.

The provider further states that users can control who can access their full profile by, for example, being able to mute a player`s communication, block further interaction with a particular user, etc. Parents or guardians also have plenty of choices to manage, and eventually, restrict their children`s experience and playing environment (both online and offline) on Xbox LIVE through the Xbox Live Family Settings and the tutorials that accompany them.

Main findings in relation to the website and console

Tools and technologies available to users on Xbox Live are designed to give the user control over online interactions in the course of gameplay or other entertainment activities. Users create profiles which may include a brief motto, personal picture of their avatar, name, bio, and location. Profiles for child accounts are invisible by default. Child account holders may only accept friend requests with parental consent. Communication, whether by text, messaging or chat is restricted to friends only. Teen accounts by default make profiles visible to friends only and also require parental approval to accept friend requests. Likewise, online communication whether by text, messaging or chat is restricted to friends only.

During the period of testing, a number of 'fake' Xbox Live accounts for both the console and website were set up to assess the extent to which access to personal information and online interaction was visible or accessible beyond a user's approved contact list of friends. Profiles of minors, registered users under the age of 18, were not accessible in either internal or external search engines. Adults registered on the site could only find the profile of minors if they know the URL. The visible profile in such instances contains only the username or gamertag, the user's avatar and game scores. Identifying information is not featured in gamer profiles though users are free to add further details in their own bio. There is no facility to post comments, pictures or other content on a user's profile as is the case for other SNS services. In the case of Xbox Live, gamers may rate other players by submitting a gamer review. Abuse of the gamer reputation feature may be deemed a violation of the code of conduct.

Xbox forums are another feature of the Xbox Live service accessed from the Xbox Live website. Participation in Xbox forums is not subject to the same online safety settings that apply for other aspects of the service and separate preferences need to be set to either allow or block communication in forum conversations. If enabled, users may join in conversations, start new threads or communicate with other members by private message. By default forum participation is enabled and in this way, it was possible for an adult – in this case a friend of a friend - to send a private message to a minor within a Community Forum. A friend request was also sent to the minor's account. Friend requests for minor accounts by default require parental approval. Parental consent is not needed for participation in Xbox forums, however, including communication with other members via private messaging.

Apart from this exception, online and console family settings proved to be robust and effective in maintaining secure settings for younger players.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

According to the self-declaration, in Xbox LIVE users can complain about a players` inappropriate behaviour or content including the use of inappropriate language or profile content, as well as actions such as cheating or griefing. The provider also claims that interactions with other users can be muted and players can be blocked. According to the provider, it is also possible to report an incident by directly selecting an offender's user

profile (e.g. another gamer) and report them in case of inappropriate behaviour. After receiving a complaint, the provider claims to review each report for accuracy. If the complaint is valid a number of actions can be taken against the offender including suspending the offender for a certain period of time or banning the offender's account and/or their console from Xbox LIVE permanently.

The self-declaration does not explicitly refer to if the procedures to report other user's content or behaviour (mechanism 2) are easily accessible or if the procedure to report inappropriate conduct or content is easily understandable for children. The self-declaration does not provide concrete information on if users are provided with an indication on if their reports are acknowledged nor information on how reports are typically handled.

Main findings in relation to the website and console

A number of mechanisms are provided to enable users report content or behaviour that violates the Terms of Service. In the course of gameplay or other online interaction, users may block communications from individual players. They can remove them as friends and/or submit player reviews. In Xbox Live Forums, accessed on the website, users may flag posts as abusive. The main way of reporting abuse on the console is through filing a complaint on a player's profile. The instructions provided on how to report and file a complaint are clear and readily accessible. In making a complaint, a user is asked to provide precise information concerning the nature of the violation. Typical violations cited include abusive communication through text or voice or video/picture communication, or tampering with the system (e.g. attempting to influence player feedback or tampered with a game or console). An option is also provided to submit a player review rather than a complaint. During the test, a sample complaint was filed using the console about another player for harassing and bullying behaviour. No difficulties were encountered and confirmation of successful submission was given. A notice was given following submission that according to its Terms of Service, XBOX Live review every complaint but will not disclose the status or results of individual complaints. Accordingly, the player who submitted the complaint had no follow up communication from the provider and did not know what effect, if any, their report had. No evident action was taken against the profile reported either.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

As stated by the provider in the self-declaration, apart from existing mechanism to report abuse, there is a complaint centre where users can report abuse on the website. Besides, the provider claims to have also "deputised certain trusted individuals" to report inappropriate content found on the service. "Their reports automatically lead to a service penalty for that offender appropriate for the severity of the offense".

Xbox LIVE`s self-declaration specifies how the provider deals with the reviewing of content and the setting of penalties for offending users. However no explicit information is provided regarding how they deal with the removing of inappropriate, offending or illegal content. Xbox LIVE claims to work "in close cooperation with law enforcement and government agencies in response to lawful request".

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

The provider states that when setting up privacy settings, users are given relevant information regarding how to control access to their profile and game play information including their gamer profile and played games. On every page of Xbox.com users can access the "Online Privacy Statement". The provider further claims that this information can also be accessed from the console. Details on the privacy policy are also available from links to the Microsoft website and can be accessed on every page of Xbox.com. The self-declaration mentions that users can control who sees their profile and game play information. For instance, users can decide who sees customizations made to their gamer profile including name, location and bio. It also specifies that when

creating a child account, parents are alerted "to the fact that their child's name, location, and bio are visible to anyone the parent allows. If they choose to make this information available to the child's friends, they can also choose to approve with whom the child can be Xbox LIVE friends".

The self-declaration does not make explicit if privacy settings are easily accessible, prominent or if they are available at all times.

Main findings in relation to the website and console

Privacy settings are an integral element of the Xbox 360 console and Xbox Live online safety settings. The Xbox Live Privacy Statement is available on each page of the website and in the Account Management panel of a user's profile on the console. Extensive controls are provided over how personal information is made visible or hidden from other players. Default settings enable maximum privacy through standard profile options for child and teen accounts. Modifications may be made which alter specific aspects of information visibility and clear instructions and guidance is provided. Online privacy settings can be accessed at any point from the user's profile on both the console and on Xbox.com and are prominently displayed. However, teens and child users require parental consent to make any changes. A parent must log in with their Windows Live ID to approve any changes to safety settings.

Users have control over the relatively limited information available in gamer profiles and are able to restrict other features such as online status and game history. Modifications to privacy settings are easily achieved which allow users to block access to their profile, to share it with friends only or to make it visible to all. By default, access to a child account profile is blocked while a teen account profile is visible to friends only. Setting privacy options for Kinect sharing also requires special attention: even if a teen account is set to friends only for video communications, users also need to set additional controls for Kinect sharing of data (videos and photos) outside of Xbox Live. This does not affect any privacy settings for communication, however. Online resources provide additional guidance on the importance of privacy controls and are strongly reinforced through safety websites such as the dedicated online safety website http://playsmartplaysafe.eu/ and Microsoft's Safety and Security Center http://www.microsoft.com/security/default.aspx. Reference to the manual or online support may be required in order to find out how to delete a profile. This is done through System Settings and selecting Gamer Profiles on the Memory tab. Once located, deletion of a user profile is straightforward and easy to manage.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

The provider claims to employ a range of automated technologies to ensure the integrity of their services. The self declaration indicates that when the provider becomes aware of a violation to their terms of use or code of conduct (e.g. through user-generated reports), they "take steps to remove and take down illegal or prohibited content/conduct". Finally, in their self-declaration Xbox Live indicates that they employ especially trained personnel on (their) global processes and standardised practices so as to ensure a consistent way of responding according to applicable laws and worldwide regulations related to this subject.

Summary of Results and Conclusions

On the website, Principles 1, 2, 3 and 6 were assessed as very satisfactorily implemented and Principle 4 as rather satisfactorily implemented. The main strengths of this SNS are the availability of targeted safety information for minors and carers. This information is practical in nature and intended to provide users with the necessary skills to use Xbox services effectively and in a safe manner. The extensive tools provided to ensure the services are age-appropriate for the different categories of users are another positive aspect. Parental control features are readily accessible, easy to set up and to manipulate. Teen accounts by default restrict profile sharing to friends only and also require parental approval to accept friend requests. Default

settings enable maximum privacy through standard profile options for child and teen accounts. Reporting inappropriate content or behaviour is easy and deleting a user profile is straightforward and easy to manage. Some areas of attention include:

- Some difficulties were encountered during the tests in locating safety resources, but once identified were found to be comprehensive and informative.
- There is little evidence of safety information specifically designed for younger children. The available resources are, however, written and presented in a very user-friendly way and are informative for new users of all ages.
- Online communication in the accounts of minors, whether by text, messaging or chat is restricted to friends only. However, despite this, it was possible for an adult – in this case a friend of a friend - to send a private message to a minor, but only within a Community Forum.
- During testing, a player submitted a complaint about another player for harassing and bullying behaviour, but they received no follow up communication from the provider and did not know what effect, if any, their report had. Furthermore, no evident action was taken against the profile reported either.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	X		
2	X		
3	X		
4		X	
5	X		
6		X	
7	X		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	X		
2	X		
3	X		
4		X	
6	X		

IMPLEMENTATION OF THE SAFER SOCIAL NETWORKING PRINCIPLES FOR THE EU
YOUTUBE

Brian O'Neill, Dublin Institute of Technology, Ireland
Verónica Donoso, Appointed Research Coordinator by the EC

Introduction

YouTube is a video-sharing website on which users can upload, share and view videos. Founded in 2005, YouTube displays a wide variety of user-generated video content, including movie clips, TV clips, and music videos, as well as amateur content such as video blogging and short original videos. Acquired by Google in 2006, YouTube is described as "the world's most popular online video community,"[26] It has over 3 billion views per day and is the third most visited website globally.[27] YouTube is now localized in 25 countries across 43 languages. While most of the content on YouTube is uploaded by individuals, media corporations and other organizations also offer video content via the site, as part of the YouTube partnership programme. Unregistered users may watch videos, and registered users may upload an unlimited number of videos, comment on other videos and create personalised channels in which to present their own content. YouTube is intended for individuals of 13 and over. Videos that are considered to contain potentially offensive content are available only to registered users 18 years old and older.

Summary of main findings

This report summarises the main findings of the tests carried on the YouTube website in the period from June 20, 2011 to June 24, 2011. A high commitment to safety on the part of YouTube was evident through the prominent way in which it is featured throughout its service. Safety information for parents, teachers and younger users is widely available and extensive resources including educational materials, safety tips and videos, help articles and a help forum are easily accessible to users. YouTube's Community Guidelines provide the principal means by which users are informed about acceptable content and behaviour on the service. These are written in admirably clear and plain language and seek to promote a respectful and common sense approach to sharing video content. Users are invited to report violations of the terms of use by flagging content that may be considered in breach of the code or inappropriate for viewers below the age of 18. Tests performed in reporting inappropriate content were found to be very effective and prompt action was taken in restricting content unsuitable for minors. Privacy settings are readily accessible to users and allow making uploaded video content private or restricted to a named group of friends as appropriate. Information contained on one's personal channel can be modified and hidden as required. The channel as a whole can be made invisible. However, there is no option to restrict its view to friends only or to discriminate between groups of friends. Once personal information is made visible, it may be viewed by all users, whether registered or unregistered.

[26] Janet Wasko and Mary Erickson (2009) 'The Political Economy of YouTube' in The You Tube Reader', Pelle Snickars Patrick Vonderau eds. Stockholm, National Library of Sweden.
[27] 'Statistics'. Retrieved from: http://www.youtube.com/t/press_statistics

Analysis of Results by Principle

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner

Main findings in relation to the self-declaration

In its self-declaration, YouTube states that they provide safety information targeted to parents, teachers and young people via two main channels: YouTube's dedicated Safety Centre and Google's Family Safety Centre. YouTube's dedicated safety centre provides users with tips such as keeping their personal videos private, protecting their online identity, managing interactions with other users on the platform, etc. It also provides videos focusing on how to stay safe online and in particular on YouTube. Google's Family Safety Centre provides additional safety tools and resources for children, teachers, parents and families (e.g. The possibility to prevent unwanted content via "SafeSearch"). The self-declaration also states that users can access the Community Guidelines, Help centre and Safety Tips from every YouTube page and that all these resources are "written in an easy to understand, user-friendly format". The self-declaration further states that YouTube has recently added the Educator and Parent Resources pages, specifically targeted at those audiences.

The signatory states that they provide clear information and guidelines ("in an easy-to-understand language") about what content is acceptable in their service and what is not. This information is made available to users via the Community Guidelines, which emphasize, for instance, that uploading inappropriate content such as hate speech, pornography, images of drug abuse, graphic violence, is forbidden. Also, predator behaviour, harassment, revealing other users` personal information, or any other activity that may endanger the safety or privacy of young users are prohibited on the site. Information about the consequences of inappropriate behaviour on the website are also mentioned in the self-declaration, for example, "users who repeatedly violate our policies will have their accounts terminated". The provider indicates that the Community Guidelines can be accessed from every YouTube page.

Main findings in relation to the website

Safety considerations are very evident across YouTube's services. The YouTube Community Guidelines – the code of conduct for using the service – as well as safety tips and access to the Help Centre are available from each page of the website. New users will find easily accessible information from the welcome page and in a series of short articles in the link called About YouTube. The You Tube Community guidelines, its code of conduct, provide a comprehensive list of prohibited content. The main areas of risk are highlighted on the You Tube Safety Centre. Users choose from a checklist of different risk areas and are provided with targeted, country-specific information. Safety information is presented in plain language and in a user-friendly format. It is easy to find and users will have little difficulty in following the instructions and information given. Resources for parents and teachers are prominently displayed in the Safety Center, again accessible from every page of the site. Parental guidance includes an easy to follow Frequently Asked Questions (FAQs) section, short tips on ensuring safety for children on YouTube, and a series of short videos on safer technology use, how to deal with cyber bullying, and implementing safety features of the service. Educator resources include further details of safety features, guidelines of flagging potentially inappropriate content, and more detailed discussion of privacy and harassment issues. A series of Help articles and a Help forum is available via the Safety link of the website and includes detailed community discussion of a wide range of safety issues.

The legal agreement between the user and the YouTube service is accessed from the bottom of each webpage. This comprises the Terms of Service, Community Guidelines – or terms of use – and the privacy policy also accessed from each web page. The Community Guidelines sets out in clear terms common sense rules about use of the service, prohibited content and behaviour and describes for users the process of reporting inappropriate content. The Community Guidelines represent a very clear, succinct statement of permitted and prohibited behaviour and conduct on YouTube. It is integrally linked to the reporting mechanism for flagging inappropriate content/violations of the code and is presented in a very easy-to-understand format. The Community Guidelines also feature a video on staying safe on YouTube.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience

Main findings in relation to the self-declaration

The self-declaration states that the minimum age requirement in order to subscribe to YouTube is 13. The provider claims that a cookie is placed on the user`s browser to prevent re-registering with a different age. The self-declaration further states that upon notification or if suspected to be younger than 13, a user`s account will be closed.

Regarding the mechanisms through which the service provider claims to ensure limited exposure to potentially inappropriate content and contact for children, YouTube claims to have implemented mechanisms that include community flagging, and porn image detection. Automated systems are employed to help classify videos based on their content and meta-data. "Where videos are determined to be unsuitable for younger viewers, such content is demoted in browse pages." Flagged videos (i.e. reported by the community) are reviewed, and not made available to minors. The self-declaration states that users younger than 18 are warned by means of an insterstitial page that they are about to watch videos that have been flagged as not appropriate for their age group. The user can then sign in stating that they are older than 18 and watch the video. The provider claims that if they have previously signed in as younger than 18 a cookie placed on their browser will prevent them from watching the video in question.

According to the self-declaration, YouTube has implemented a number of measures including: Safety Mode that allows users to choose not to see "potentially objectionable content they may find offensive" and also to continually develop innovative tools to keep the members of their community safe. The provider also claims to employ digital hashing technologies to prevent the re-upload of files that have been removed from the site for violating the sites` Community Guidelines while YouTube Safety Mode allows users to choose not to see "potentially objectionable content they may find offensive".

Main findings in relation to the website

The minimum age required to use YouTube is 13. Under-13 year olds are blocked from registering on the site. A cookie placed on the user's browser prevents an underage user from attempting to re-register on the site with an older birth date. In testing, this was found to be effective and registration for a 9 year old was denied even when the age was changed to over 13. On removing cookies from the computer used, it was, then possible to register as an older user. Email verification was all that was required for successful registration. According to the self-declaration, content that is deemed by the YouTube community to be inappropriate for under 18 year old viewers is restricted. Unregistered viewers have to sign up and confirm they are over 18 to access any content flagged as adult. In tests, it was confirmed that a registered user below the age of 18 is denied access. In order to prevent minors accessing potentially inappropriate content, YouTube advocates the use of its Safety Mode. Safety Mode is a setting, accessible on the bottom of each webpage. It filters content that may be found to be offensive, even though it is not against YouTube's Community Guidelines or has not been flagged as adult. With Safety Mode enabled, the filtering of age restricted content was found to be effective. It does not show up in video search, related videos, playlists, shows and movies. It is an 'opt in' setting, however, and is not enabled as a default on the accounts of minors. As an additional parental control, the Safety Mode may be locked for a particular browser to ensure that it can't be switched off by minors using that computer.

Principle 3: Empower users through tools and technology

Main findings in relation to the self-declaration

Regarding the tools and technologies employed by the service provider in order to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted content or conduct, the provider claims to provide users with "a variety of tools and advice to help them protect their privacy and to control how others interact with their videos". These options include, among others, the possibility to control how others interact with their videos, the possibility to prevent others from embedding one`s videos on 3rd party pages and the option to pre and post-moderate comments on videos.

According to the provider, users can also choose to only share a video among a certain number of friends or family members. YouTube further claims that users have channels instead of profile pages. These channels display the user names, but not real ones. One advantage of these channels would be that they allow users to post/exchange videos without necessarily having to disclose much personal information. According to YouTube's self-declaration, "YouTube does not have profile pages in the same way as social networking services. (…) YouTube is a platform for exchanging user created content rather than sharing a social profile of one`s self". However, if users wish so, they may add personal information to their profiles. It is not clear from the self-declaration, though, if this information is (automatically) mapped into the user's profile[28] and, thus, visible to other (registered and/or on-registered) users.

Main findings in relation to the website

Users of YouTube have a number of tools and technologies available to them to manage their experience of the service. The aforementioned Safety Mode, when switched on (it is set to off by default), will filter potentially inappropriate content from searches and playlists. Content flagged through YouTube's reporting service will also be inaccessible to account holders under the age of 18 even if Safety Mode is not enabled. The provider in its Self Declaration notes that YouTube does not have profile pages in the same way as a social networking service. However, 'Channels' created by users can act very much like an SNS profile. Primarily designed to present uploaded videos and to display playlists of other YouTube content, a user's channel can be personalised with a variety of information including name, personal interests, hometown, etc. It also contains a list of friends and subscribers to the channel; it includes comments posted on the channel by other users; statistics relating to the channel and video views; and a record of recent activity by the user.

Users are given full control over the information made available or not on their channel, but any information displayed is visible to everyone, registered or unregistered. In a sample account for a minor set up for the purposes of testing, there was no difference in the amount of information visible on the channel to friends and other minors, to other adults or to unregistered users. Default privacy settings make the channel visible to all. In addition, while adding (or editing) information to the channel, users are not warned that this information would be made publicly available to other YouTube users. However, an instruction is permanently available stating that: "Your channel viewers will see links here, including "subscribe" and "add as friend"." All users are allowed by default to send and receive messages and to comment on videos. Information about a user's favourites, subscriptions and friends list are also set to be viewable by all as a default setting. When uploading video clips (or recording from a webcam) users are presented with a set of broadcasting and sharing options. By default, sharing of video content is set to public so that anyone can search for and view content. Uploaded content may also be set to unlisted, meaning that it does not appear on public spaces on YouTube (in search or on a user's channel) but may be viewed by anyone with the link. A third option is to restrict videos to private viewing so that only those given permission can access them. Comments may also be pre-moderated or restricted to friends only. Additional tools available to the user include the ability to remove comments and report as spam and to block unwanted messages/other users. During the tests, restricting uploaded videos to private viewing proved to be effective: only users who had been given permission were able to access uploaded content and it was not possible to locate it in search.

[28] According to the provider, although not explicitly stated in the self-declaration, any personal information provided during the account registration process is not publicly displayed by default. The registration process requires the following information: Username, E-mail, Date of birth, and Gender.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service

Main findings in relation to the self-declaration

YouTube claims to have developed a community policing system so that users can "flag" potentially inappropriate or illegal content that violates the Community Guidelines. Users can select the "Flag" link whenever they encounter inappropriate content. Flagged videos are promptly reviewed by dedicated YouTube staff working 24/7. Specific instructions and guidance on how to report inappropriate or illegal content are found in the Help Centre. The self-declaration states that users can also directly contact YouTube via the Help & Safety Tool to report policy violations or they can directly report issues to local organisations such as Suicide Hotline or the National Centre for Missing and Exploited children (NCMEC) whose contact information is made available via the Safety Resources section.

No information on if users are provided with an indication if their reports are acknowledged nor information on how reports are typically handled was found in the self-declaration. The self-declaration does not explicitly mention if the procedure to report inappropriate conduct or content is easily understandable for children or if it is age-appropriate, although it does indicate that the reporting tools provided "are designed to be self-explanatory and are easy to find".

Main findings in relation to the website

YouTube's most prominent mechanism used to report abuse or material that violates the terms of use is the "flag" link available below the viewing window for each video. The flag is an easy to use way to report offensive or inappropriate content and offers a simple two step process for users to request a review by YouTube staff. The Community Guidelines provide clear instructions and information about what happens when a video gets flagged and confirms that flagged videos are not automatically taken down by the system. In this test, a video depicting drug use, visible to a minor, was flagged. No problems were encountered in filing the complaint and an acknowledgement of receipt was given. Within a short time, approximately 4 hours, the video had been age restricted. A query about how to report content was also posted on the Help Forum and a reply was promptly received. Users can also report privacy or harassment complaints and other policy violations through the Help & Safety Tool. This is accessed through the Safety link at the bottom of each page. A Privacy complaint process through an anonymous web-form allows any viewer to file a complaint against another user for harassment or privacy violation. Users are asked to describe the nature of the violation and to provide the username of the offender. Policies on safety issues and instructions about the complaints procedure are comprehensively covered in the Help section. Policy enforcement in relation to sexual or violent content, videos involving minors, and policies on account strikes and account termination are provided.

Principle 5: Respond to notifications of illegal content or conduct

Main findings in relation to the self-declaration

Regarding the mechanisms employed by the provider in order to respond to notifications of illegal content or conduct, YouTube claims that when they become "aware that a video violates the law, YouTube cooperates with law enforcement agencies to deal with the video *quickly* and in the proper legal framework". For instance, certain types of content such as child pornography are reported directly to the National Centre for Missing and exploited Children (NCMEC). The self-declaration further emphasizes that when content is flagged or reported through the Help & Safety Tool, it is reviewed "expeditiously and dealt with appropriately". Besides, the provider states that via the Safety Resources, users can directly report issues to local organisations such as Suicide Hotline, NCMEC, etc.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy

Main findings in relation to the self-declaration

The self-declaration states that users of this SNS are provided with a range of privacy setting options including the possibility for users to make their channel private, the option to share videos privately with a limited number of people or to remove their videos from public listings, etc. Advice and guidelines on how to protect their online identity and privacy are provided to users in the Safety Tips accessible from every page and when setting up an account.

The self-declaration mentions that, basically, no personal information provided during registration is mapped onto the user`s profile. "The default information on a users channel shows the user name, not their actual name." After registration, and only if they wished so, users can add some personal information on their channel.

Main findings in relation to the website

Privacy settings allow users to select which 'modules' on their channel to make visible and to edit or restrict the information displayed. According to the company's statement on Principle 6, YouTube provides an option for users to make their channel private. What this means is that users have the option to either make their channel visible or invisible. There is no option to restrict a channel view to friends only. Once a channel is made visible, it is available to all users, registered or unregistered. The default setting for all account holders including minors is to make the channel and the information visible. Users have to deselect options to hide or restrict information. This means that actions taken by a user on YouTube such as favoriting, liking, or uploading a video will be visible to all unless de-selected. These actions appear as a 'feed' in the Recent Activity box on each user's channel. Privacy settings for activity sharing may be accessed directly alongside the Recent Activity box in which users choose which information they wish to share. The activity feed may also be connected to external accounts such as Facebook or Twitter if desired. Users may also restrict others from adding comments to a user's channel. By default, everybody can comment. A setting to pre-moderate comments can be enabled and/or to restrict commenting to friends only.

Slightly different privacy controls are available for uploaded video content. By default, uploaded videos are public. Videos appear on one's channel and also in lists across YouTube. They may also be set to unlisted so that they don't appear in search but may be viewed by anyone with the link. Alternatively, videos may be set to private, so that they are viewable only by named contacts. Videos with restricted privacy settings do not appear on a user's channel.

Privacy settings that control how personal information is made available across the website, as for example as listed within individual video clips, are also accessed via the user's channel. Within an account settings option, users manage whether statistics or data for videos are displayed with video content or whether friends and subscriptions lists will be visible. By default, information is publicly visible and the user must opt out to hide the information. It is also possible to opt out of personalised advertising based on a user's search history. A privacy statement is accessible on each webpage and a link is provided to the general Google Privacy Policy. A range of resources is provided in the Help section and in the community forum. A help article on 'Editing your channel for privacy' listed in the privacy statement was not available though a search of the Help Centre reveals additional information on managing privacy. Deletion of a profile and a user account is easy to accomplish and users are informed that their content will be deleted and no longer available.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct

Main findings in relation to the self-declaration

As mentioned under Principles 2 and 5, and as stated in the self-declaration, YouTube employs automated tools such as filtering and porn image detection as well as human forms of moderation such as community flagging

to report potentially inappropriate or illegal content. The provider claims that every flagged video is promptly reviewed. Users can also directly contact YouTube via the Help & Safety Tool to report policy violations or they can directly report issues to local organisations such as the National Centre for Missing and Exploited children (NCMEC). The self-declaration further indicates that the support team reviews the videos 24/7 to make sure there is no inappropriate content available on the site.

Summary of Results and Conclusions

On the website, all the Principles were assessed as very satisfactorily implemented. The main strengths of this SNS are safety information for parent, teachers and younger users is widely available and extensive resources including educational materials; safety tips, etc. are easily accessible to users. YouTube's Community Guidelines are written in admirably clear and plain language and seek to promote a respectful and common sense approach to sharing video content. Other positive aspects include the fact that reporting abuse on the platform is easily available and efficient. Ready access to privacy settings by clicking on the user's channel was found to be very user-friendly, effective and easy to manipulate while deletion of a user account is easy to accomplish and users are informed that their content will be deleted and no longer available.

Some areas of attention include:

- Default privacy settings make a channel visible to all, including unregistered users. All users are allowed by default to send and receive messages and to comment on videos. Information about a user's favourites, subscriptions and friends list are also set to be viewable by all as a default setting.
- Even though YouTube states in its self-declaration that users' profile pages (channels) are not used in the same way as other social networking services, if users wish so, they can add (plenty of) personal information to their channels. It is also true that YouTube users are given full control over the information made available or not on their channel, however any information uploaded is visible to everyone, including both registered and unregistered users.
- Information contained on one's personal channel can be modified and hidden as required and user channels as a whole can be made invisible. However, there is no option to restrict its view to friends only or to discriminate between groups of friends.
- The default setting for all account holders including minors is to make information contained on a user's channel visible. Users have to deselect options to hide or restrict information.
- Safety Mode, is not switched to on by default.

Assessment of the Principles in the Self-declaration

Principle	*Very satisfactory*	*Rather Satisfactory*	*Unsatisfactory*
1	x		
2	x		
3		x	
4		x	
5	x		
6		x	
7	x		

Implementation of the Self-declaration on the SNS website

Principle	*Very satisfactory*	*Rather satisfactory*	*Unsatisfactory*
1	x		
2	x		
3	x		
4	x		
6	x		

FOR FURTHER INFORMATION:
DIRECTORATE-GENERAL
INFORMATION SOCIETY AND
MEDIA
EUROPEAN COMMISSION
SAFER INTERNET PROGRAMME
E-MAIL:
SAFERINTERNET@EC.EUROPA.EU
FAX: + 4301 34079
OFFICE: EUFO 1194
EUROPEAN COMMISSION
L-2920 LUXEMBOURG

http://ec.europa.eu/saferinternet